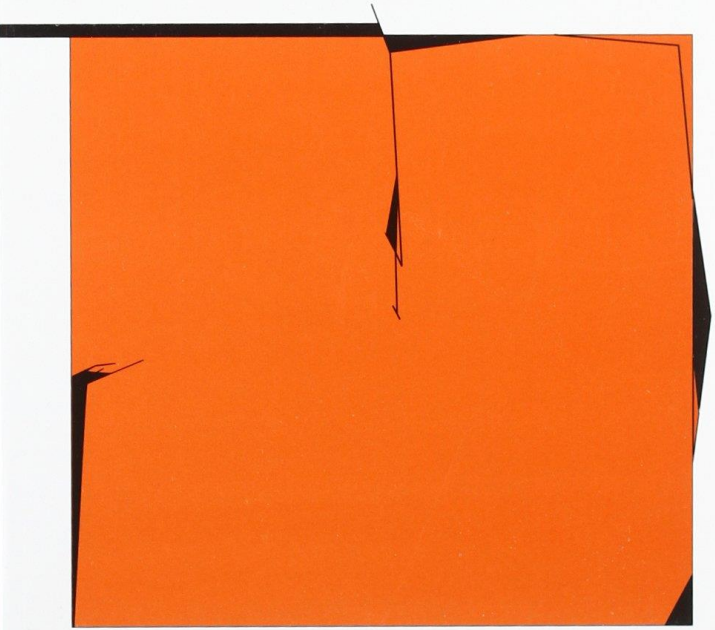
APORTACIONES MATEMÁTICAS

TEXTOS **32**
NIVEL MEDIO

INTRODUCCIÓN A LA TEORÍA DE GRUPOS

FELIPE ZALDÍVAR

PRIMERA REIMPRESIÓN



SOCIEDAD MATEMÁTICA MEXICANA

2009

UNIVERSIDAD NACIONAL DE INGENIERIA
FACULTAD DE CIENCIAS
BIBLIOTECA

INGRESO
Fecha 05/02/08
Nº 09511

COMPRA "SAN CRISTOBAL" O/C 60833 S/. 78.00
DONACION
CANJE

Felipe Zaldívar
Departamento de Matemáticas
Universidad Autónoma Metropolitana-I
09340 México, D. F.
MÉXICO

Compra : "SAN CRISTOBAL" O/C 60833 S/ 78.00 (05/02/08)

APORTACIONES MATEMÁTICAS

Comité Editorial:

Marcelo Aguilar
IM, UNAM

Luz de Teresa
IM, UNAM

José Ma. González Barrios
IIMAS, UNAM

Luis Gorostiza
CINVESTAV

Max Neumann
IM, UNAM

Guillermo Pastor
ITAM

Raúl Quiroga
CINVESTAV

Sergio Rajsbaum
IM, UNAM

José Seade
IM, UNAM

Martha Takane
IM, UNAM

Jorge X. Velasco
UAM, Iztapalapa

Editores Ejecutivos:

Luis Gorostiza
CINVESTAV
lgorosti@math.cinvestav.mx

Luz de Teresa
Instituto de Matemáticas, U
deteresa@matem.unam.mx

Publicación de la
SOCIEDAD MATEMÁTICA M
REVERTÉ EDICIONES, S.A. D

ISBN: 968-36-3591-1 (Aportaciones Matemáticas
ISBN: 968-36-3594-6 (Serie Textos)
ISBN: 970-32-3871-8
ISBN: 968-6708-66-9 (Reverté Ediciones, S.A. de C.V.)

Printed in Mexico / Impreso en México

Índice general

Introducción		v
Capítulo 1.	Simetrías y operaciones binarias	1
Capítulo 2.	Grupos y subgrupos	11
Capítulo 3.	Grupos cíclicos	21
Capítulo 4.	Grupos de permutaciones	29
Capítulo 5.	Clases laterales y grupos cociente	53
Capítulo 6.	Homomorfismos e isomorfismos	71
Capítulo 7.	Productos directos y grupos abelianos finitos	87
Capítulo 8.	Acciones de grupos y un teorema de Frobenius	97
Capítulo 9.	Los teoremas de Cauchy y Sylow	107
Capítulo 10.	Grupos simples	131
Capítulo 11.	Grupos solubles	139
Capítulo 12.	Grupos de matrices	159
Capítulo 13.	Representaciones lineales de grupos finitos	169
Capítulo 14.	Caracteres de grupos finitos	185
Capítulo 15.	Aplicaciones de la teoría de caracteres	209
Apéndice A.	Enteros algebraicos	235
Bibliografía		251
Índice alfabético		255

Introducción

La teoría de grupos está donde está la acción

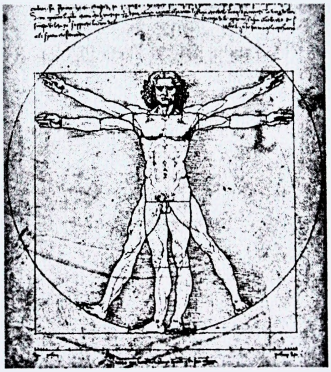
EN EL PRINCIPIO FUERON PERMUTACIONES de raíces de polinomios, como en Galois, o permutaciones de cualquier conjunto finito, como en Cauchy. Todos los primeros practicantes trabajaban con grupos de permutaciones hasta que el final del siglo XIX los alcanzó y Frobenius ya estaba listo para definir un grupo abstracto por medio de una lista de axiomas. Además de los grupos de permutaciones, la Geometría, como la entendió Klein, aparece en este contexto y encontramos grupos actuando sobre objetos geométricos y una geometría se define por los objetos invariantes bajo la acción dada. En nuestros días la teoría de grupos va de lo abstracto a lo extremadamente concreto —cálculos en computadoras— pero siempre reteniendo su meta inicial: el estudio de la simetría en todos los contextos, desde grupos cristalográficos hasta grupos de Lie asociados a ecuaciones diferenciales, desde la combinatoria hasta la teoría de números, desde la geometría hasta la física, donde quiera que hayan simetrías, la teoría de grupos está presente. Este libro es una introducción a la teoría de grupos, y a pesar que sólo es una introducción elemental, toca muchos aspectos de la teoría, con un énfasis en los grupos finitos, preparando al estudiante para niveles más avanzados. He tratado de bosquejar algo de la historia de la teoría de grupos, refiriendo en las notas al final de cada capítulo a las fuentes apropiadas, recordando el origen de algunos de los conceptos y teoremas. La bibliografía también incluye libros y monografías, desde textos elementales como el presente, hasta monografías avanzadas, donde el estudiante puede ver otros enfoques o continuar su estudio de la teoría de grupos. Los prerequisitos para leer este libro se han mantenido a un mínimo: un curso de Álgebra Lineal y un curso de Matemáticas Finitas que incluya algo de divisibilidad de enteros, números primos y el teorema fundamental de la aritmética. El libro comienza con un intento de describir el concepto de *simetría* para motivar la idea de *grupo* y después de discutir algunos ejemplos importantes, grupos *cíclicos*, de *permutaciones* y de *matrices*, introduce los teoremas de estructura básicos, desde el teorema de Lagrange hasta los teoremas de Sylow, y luego los aplica para dar una introducción elemental al estudio de los grupos *simples* y *solubles*. La parte final del libro usa álgebra lineal combinada con teoría de grupos introduciendo al lector a la teoría de representaciones de grupos finitos y luego aplica estos resultados para probar un importante teorema de Burnside, a saber, que todos los grupos finitos cuyos órdenes son de la forma $p^a q^b$, con p, q primos, son solubles. La demostración de este teorema usa algunos resultados sobre enteros algebraicos de los cuales se dan demostraciones elementales en el Apéndice y que, adecuadamente, usan polinomios simétricos. Podría decirse que hay una cierta simetría en la forma en que el libro se desarrolla ya que, comenzando con una noción intuitiva de la noción de simetría, termina con una aplicación que involucra el uso de polinomios simétricos

cuyo origen puede ubicarse en uno de los inicios del Álgebra misma, a saber el estudio de las permutaciones de las raíces de polinomios, por Galois, Lagrange y Viète.

Capítulo 1

Simetrías y operaciones binarias

LA IDEA DE SIMETRÍA ESTÁ presente en varios contextos: en las artes plásticas (pintura, escultura, arquitectura), donde en algunos casos es obvia, por ejemplo, en el diseño de algunas construcciones—iglesias o catedrales con sus dos torres, acueductos con sus arcos repetidos, etc. Un ejemplo inmediato está dado por las simetrías de la figura humana, como es manifiesto en el conocido dibujo de Leonardo da Vinci sobre las proporciones del cuerpo humano:



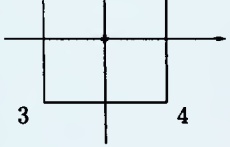
Es fácil encontrar ejemplos, en las artes plásticas, de cómo el artista aprovecha la simetría para crear objetos de arte. Los frisos de Mitla en Oaxaca, o las decoraciones de edificios construidos por los árabes en la España morisca comparten una misma fuente geométrica. Sin embargo, aunque no tan obvio como en los ejemplos anteriores, también la idea de simetría está presente en otra de las artes: en la música, por ejemplo en el contrapunto (fugas especulares, cánones, etc.). El lector puede pensar en cómo la idea de simetría también se usa en la literatura, en ocasiones en forma sutil. Ahora, una vez convencidos de la ubicuidad de la idea de simetría, su aparente simplicidad no ayuda

a entenderla, es decir, ¿cómo podríamos definir el concepto de *simetría*, que aparentemente es claro y evidente hasta que pensamos en cómo definirlo, y en ese momento se vuelve elusivo y ya no es tan evidente?

Un primer enfoque sería pensar a un *objeto simétrico* como aquel objeto que *no cambia* cuando lo *movemos* de unas ciertas formas. Para comenzar debemos aclarar que *mover* no necesariamente quiere decir movimiento en el sentido físico. Por ejemplo en la música no movemos las notas musicales. O en literatura no movemos las palabras o imágenes o metáforas. Quede claro entonces que la idea de *mover* es en el sentido abstracto y en un cierto sentido querrá decir *cambiar*. Pero ¡cómo es esto!, podríamos exclamar, cómo es esto de querer definir un objeto simétrico diciendo que es aquel objeto que no cambia cuando lo movemos, es decir, ¡cuando lo cambiamos! Esta supuesta definición más parece un ejemplo de *gatopardismo* que una definición propia. Más vale entonces que comencemos a aclarar los términos que usaremos.

Lo primero que debemos observar es que el *movimiento* o *cambio* es algo que infligimos en un objeto dado. Esto implica que al objeto lo sujetamos a cierta *acción* (de nuevo, aclarando que esto no necesariamente es en el sentido físico). También es importante aclarar que los *objetos* que sujetaremos a estas acciones, tampoco necesariamente son objetos físicos y en muchos casos sólo son objetos abstractos de nuestra imaginación (qué otra cosa son las imágenes poéticas, o las figuras geométricas—acaso, ¿alguna vez hemos encontrado un triángulo equilátero en el mundo físico?). Veamos un ejemplo donde las simetrías sean fáciles de observar:

Ejemplo 1. Consideremos un cuadrado centrado en el origen de $\mathbb{R}^2$, con lados paralelos a los ejes coordenados y de lado 2:



con vértices etiquetados por 1, 2, 3 y 4. Si queremos *ver* las simetrías de este cuadrado, lo que deseamos es ver cuáles movimientos o cambios llevan al cuadrado en sí mismo. Lo primero que observamos es que basta ver qué movimientos o cambios llevan un vértice en otro ya que esto es suficiente para que el cuadrado *no cambie*. Las *acciones* sobre el cuadrado, que lo mantienen sin cambio son:

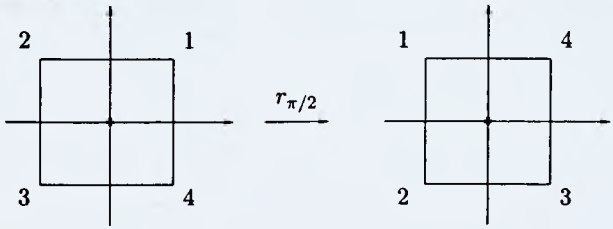
- *Rotaciones* r_θ por ángulos $\theta = \pi/2,\ \pi,\ 3\pi/2,\ 2\pi$, etcétera. En general, *rotaciones por ángulos que son múltiplos enteros de* $\pi/2$. Note que al rotar 2π es lo mismo que rotar 0 grados, También, si $n \geq 0$ es un entero, al rotar $n\pi/2$

basta considerar rotaciones para $n = 0, 1, 2, 3$ ya que los otros ángulos repiten las ubicaciones de los vértices del cuadrado. Para enteros $n < 0$, dejamos como un ejercicio mostrar que las rotaciones r_θ para $\theta = 0, \pi/2, \pi, 3\pi/2$ *generan* todas las otras rotaciones que mantienen sin cambio al cuadrado. Así, básicamente hay 4 rotaciones que dejan *invariante* al cuadrado considerado.

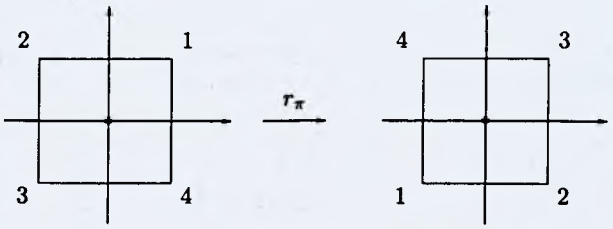
- *Reflexiones* con respecto a los ejes coordenados X y Y y con respecto a las dos rectas a 45 y 135 grados por el origen de $\mathbb{R}^2$. Hay 4 reflexiones: con respecto al eje X, denotaremos la reflexión correspondiente por ρ_X. Con respecto al eje Y, tenemos la reflexión ρ_Y. Con respecto a la recta a 45 grados, denotaremos a la reflexión por ρ_1 y con respecto a la recta a 135 grados, tenemos la reflexión ρ_2.

Veamos cómo son las *acciones* anteriores (rotaciones y reflexiones actuando sobre el cuadrado que estamos considerando, al que denotaremos por $\mathcal{C}$).

- Para la rotación r_0, esta acción no hace nada. Le llamaremos la *acción neutra o identidad* y la denotamos mediante el símbolo e.
- Para la rotación $r_{\pi/2}$, la acción sobre el cuadrado $\mathcal{C}$ está dada por:



- Para la rotación r_π, su acción sobre el cuadrado $\mathcal{C}$ es:



y notamos que $r_\pi = r_{\pi/2} \bullet r_{\pi/2}$, es decir, rotar 180 grados es lo mismo que rotar primero 90 grados y luego rotar otros 90 grados. Usaremos la abreviación

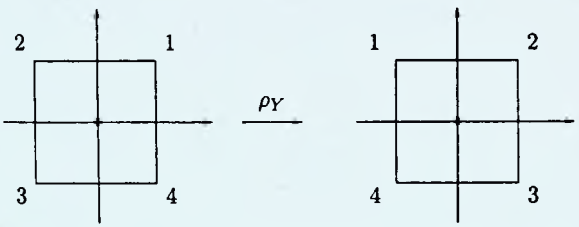
$$r_\pi = r_{\pi/2} \bullet r_{\pi/2} = r_{\pi/2}^2$$

para indicar la rotación $r_{\pi/2}$ aplicada dos veces.

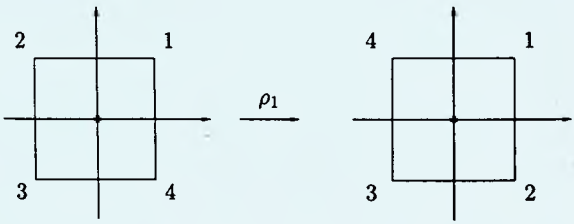
- El lector puede ver cómo es la acción de $r_{3\pi/2}$ y observar que

$$r_{3\pi/2} = r_{\pi/2}^3.$$

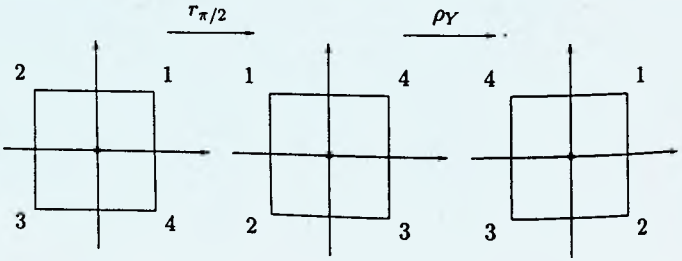
- También, observe que $r_{\pi/2}^4 = e$, ya que rotar 360 grados tiene el mismo efecto que no hacer nada.
- Para la reflexión ρ_Y, su acción sobre el cuadrado $\mathcal{C}$ está dada por:



- El lector puede ver cómo actúan las otras reflexiones. En particular, observe que la acción de la reflexión ρ_1 sobre el cuadrado $\mathcal{C}$ es:



y si consideramos la acción $r_{\pi/2}$ seguida por la reflexión ρ_Y, a la que denotamos por $\rho_Y \bullet r_{\pi/2}$, la acción correspondiente es:



y observamos que la acción ρ_1 es lo mismo que la acción $\rho_Y \bullet r_{\pi/2}$. Esto lo denotamos como

$$\rho_1 = \rho_Y \bullet r_{\pi/2}.$$

En el ejercicio 1 se pide identificar a las otras reflexiones en términos de la rotación $r_{\pi/2}$ y de la reflexión ρ_Y.

Unos cálculos sencillos nos convencerán que las simetrías del cuadrado $\mathcal{C}$ están dadas por las acciones

$$G = \{e, r, r^2, r^3, \rho, \rho \bullet r, \rho \bullet r^2, \rho \bullet r^3\},$$

donde e es la *acción neutra* que no hace nada, $r = r_{\pi/2}$ y $\rho = \rho_Y$.

Simetrías. La discusión anterior nos lleva a las ideas siguientes, que son necesarias para entender el concepto de simetría. Se tiene un conjunto de *objetos* (que puede ser uno solo, como en el ejemplo del cuadrado anterior) al que denotamos mediante A. También se tiene un conjunto no vacío G, cuyos elementos llamaremos *simetrías*, junto con una función

$$G \times A \to A$$

que asigna a cada par ordenado (σ, a), con $\sigma \in G$ y $a \in A$, el objeto $\sigma * a \in A$. A esta función la llamaremos una *acción* de G en A. Estos dos conjuntos y la acción que estamos denotando por $*$ deben satisfacer las propiedades siguientes:

(1) Para cada elemento $\sigma \in G$ y cada objeto $a \in A$ se tiene que, la acción de σ en a, denotada $\sigma * a$ es otro objeto de A.

(2) Debe haber una manera de *operar* o *componer* dos elementos cualesquiera de G, es decir, si σ y τ son dos elementos de G, debe existir otro elemento $\sigma \bullet \tau$ en G. También, el conjunto G debe contener un elemento e que funcione como la *identidad*, es decir, que compuesto con cualquier otro elemento de G no le haga nada. Hay otras propiedades de la operación de G que también necesitaremos, pero tendremos que esperar hasta el siguiente capítulo para hacerlas explícitas y por el momento sólo pensemos que G y su manera de operar $\bullet$ se parecen mucho al conjunto de simetrías del cuadrado del ejemplo 1.

(3) Al considerar dos elementos $\sigma, \tau \in G$, la composición $\sigma \bullet \tau \in G$ actúa sobre el objeto $a \in A$, en la forma natural, es decir, primero actúa τ para obtener el objeto $\tau * a \in A$ y luego actúa σ en $\tau * a \in A$ para obtener el objeto $\sigma * (\tau * a) \in A$. Es decir,

$$(\sigma \bullet \tau) * a = \sigma * (\tau * a).$$

Con esto a la mano, podemos ya definir el concepto de *simetría*. Dado un objeto $a \in A$, diremos que *tiene simetrías* (o que es simétrico) si existe un conjunto no vacío G y existen algunos elementos $\sigma \in G$ tales que dejan invariante al objeto a, es decir,

$$\sigma * a = a.$$

Los elementos de G que dejen el objeto $a \in A$ invariante, se llaman las *simetrías* del objeto $a \in A$. Note que el elemento neutro $e \in G$ siempre deja invariantes a todos los objetos $a \in A$, es decir,

$$e * a = a.$$

Así, en la definición anterior se sobreentiende que un objeto tiene simetrías si tiene simetrías diferentes de la neutra.

Operaciones binarias. En el conjunto G hemos pedido que se tenga una manera de *componer u operar* sus elementos. Es decir, dados σ y τ en G, debe existir otro elemento $\sigma \bullet \tau$ en G. Dicho en otras palabras, se debe tener una función

$$\bullet : G \times G \to G$$

a la que denotamos mediante $(\sigma, \tau) \mapsto \sigma \bullet \tau \in G$. Note que por definición de función, para el caso de la función $\bullet$ se tiene que para todos los pares (σ, τ) con $\sigma, \tau \in G$, se debe tener que $\sigma \bullet \tau \in G$. Todavía se suele decir que la operación $\bullet$ es una *operación cerrada* para indicar que cada vez que se operan dos elementos de G se obtiene otro elemento de G. También, a la operación se le llama una *operación binaria* porque asigna un elemento de G a cada *par* de elementos de G. Así, podrían haber *operaciones ternarias* que asignan a cada *terna* ordenada de elementos de G otro elemento de G. Similarmente se tendrían operaciones n-arias, para cada $n \geq 1$ entero. Desde el punto de vista del álgebra, todas estas operaciones son importantes y necesarias. Sin embargo, para nosotros, en este curso, nos interesan las operaciones binarias (y las unarias (1-arias), como veremos en un momento) y para poder operar con ternas o cuaternas o n-adas de elementos de G pediremos que la operación binaria que tenemos se pueda calcular asociando los elementos de la n-ada correspondiente en parejas. Por ejemplo, si tenemos la terna ordenada (α, β, γ) de elementos de G, para poder operar con esta terna, manteniendo el orden en que están los elementos de la terna, los podemos *asociar* como sigue:

Podemos juntar los dos primeros y luego operar con el tercero: $(\alpha \bullet \beta) \bullet \gamma$

ó podemos juntar los dos últimos y luego operar con el primero: $\alpha \bullet (\beta \bullet \gamma)$.

Observe que, en principio no hay nada que garantize que los elementos de G, obtenidos anteriormente, sean iguales. Nosotros pediremos que siempre se tenga la igualdad

$$\alpha \bullet (\beta \bullet \gamma) = (\alpha \bullet \beta) \bullet \gamma$$

para todos los elementos α, β, γ de G. Diremos entonces que la operación binaria $\bullet$ es *asociativa.*

Ejemplo 2. Si tomamos como conjunto G al conjunto de números enteros $\mathbb{Z}$, la *suma* de dos enteros es una operación binaria:

$$+ : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z} \quad \text{dada por} \quad (a, b) \mapsto a + b$$

ya que a cada par de enteros (a, b) le corresponde un único entero $a + b \in \mathbb{Z}$. El lector debe recordar que la suma de enteros es asociativa:

$$a + (b + c) = (a + b) + c,$$

para cualesquiera $a, b, c \in \mathbb{Z}$.

Ejemplo 3. Si tomamos como conjunto G al conjunto de números naturales $\mathbb{N}$, la función

$$\star : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$$

dada por $a \star b := ab$, es una operación binaria asociativa.

Ejemplo 4. Si tomamos como conjunto G al conjunto de números naturales $\mathbb{N}$, la resta dada por $(a, b) \mapsto a - b$ no es una operación binaria en $\mathbb{N}$ ya que no siempre es *cerrada*, por ejemplo, $7 - 2 \notin \mathbb{N}$.

Ejemplo 5. Si tomamos como conjunto G al conjunto de números naturales la función $\star : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ dada por $a \star b := a^b$ es una operación binaria no asociativa, ya que, por ejemplo,

$$2 \star (3 \star 2) = 2 \star (3^2) = 2^9 = 512 \quad \text{pero} \quad (2 \star 3) \star 2 = (2^3) \star 2 = 8^2 = 64$$

y así $2 \star (3 \star 2) = 512 \neq 64 = (2 \star 3) \star 2$.

Conmutatividad. Note que en el ejemplo 2, para cualesquiera dos enteros $a, b \in \mathbb{Z}$ se tiene que $a + b = b + a$. Algo similar sucede en el ejemplo 3, para cualesquiera dos naturales $a, b \in \mathbb{N}$ se tiene que $ab = ba$. Sin embargo, en el ejemplo 5, tomando $a = 2$ y $b = 3$ en $\mathbb{N}$ se tiene que $2 \star 3 = 2^3 = 8$ y esto no es igual a $3 \star 2 = 3^2 = 9$.

Cuando se tenga una operación binaria $* : G \times G \to G$ que satisfaga que

$$a * b = b * a \quad \text{para todo } a, b \in G,$$

diremos que la operación $*$ es *conmutativa.*

Los ejemplos 2 y 3 son de operaciones conmutativas y el ejemplo 5 es una operación no conmutativa.

Elemento neutro. En el mismo ejemplo 2, para el entero $0 \in \mathbb{Z}$ se tiene que $a + 0 = a = 0 + a$, para cualquier $a \in \mathbb{Z}$. Similarmente, para el ejemplo 3 se tiene que $a \cdot 1 = a = 1 \cdot a$, para todo $a \in \mathbb{N}$. Sin embargo, para el ejemplo 5 se tiene que:

$a \star 1 = a^1 = a$, para todo $a \in \mathbb{N}$, pero no se tiene que $1 \star a = a$ para todo $a \in \mathbb{N}$, por ejemplo $1 \star 2 = 1^2 = 1 \neq 2$.

Cuando se tenga una operación binaria $\bullet : G \times G \to G$ para la cual existe un elemento $e \in G$ tal que

$$a \bullet e = a = e \bullet a \quad \text{para todo } a \in G,$$

diremos que la operación $\bullet$ tiene como *neutro* al elemento e.

En los ejemplos 2 y 3 los neutros son el 0 y el 1, respectivamente. Para el ejemplo 5, el elemento $1 \in \mathbb{N}$ sólo funciona como neutro cuando lo ponemos a la izquierda, pero no lo es cuando lo ponemos a la derecha.

Ejemplo 6. Para el conjunto G de rotaciones del cuadrado, la rotación r_0 por un ángulo de cero grados es neutra para la operación $\bullet$ de G.

Notas. *Bien proporcionado*, es como en el lenguaje cotidiano nos referimos a un objeto simétrico; *bien equilibrado* o *bien balanceado*, pueden ser usados en forma equivalente y todos estos términos, de alguna forma u otra, invocan la *armonía* de las proporciones o ingredientes que percibimos del objeto en cuestión. Así, en la conducta diaria suele también invocarse el precepto aristotélico del *justo medio* hacia el cual deben tender las acciones virtuosas, según la *Ética a Nicómaco*. Para una introducción al estudio del concepto geométrico de simetría, bilateral, rotacional, traslacional y ornamental, el libro de Weyl [18] es una referencia clásica.

EJERCICIO 1. Muestre que las reflexiones ρ_X y ρ_2 se obtienen a partir de la rotación $r_{\pi/2}$ y la reflexión $\rho = \rho_Y$, en el ejemplo discutido anteriormente. Concluya que las simetrías del cuadrado están dadas, en efecto, por

$$G = \{e, r, r^2, r^3, \rho, \rho \bullet r, \rho \bullet r^2, \rho \bullet r^3\},$$

(decimos que r y ρ son las *simetrías generadoras* de G).

EJERCICIO 2. Considere un triángulo equilátero centrado en el origen y con base paralela al eje X. Obtenga sus simetrías geométricas. Simplifique, como en el caso del cuadrado listando las simetrías *generadoras*. Haga lo mismo para un pentágono y un hexágono, ambos regulares, centrados en el origen y con base paralela al eje X.

EJERCICIO 3. El lector cuidadoso habrá notado que no hemos hablado de la *simetría en la naturaleza*. Investigue al respecto y escriba un ensayo de 2 o 3 páginas al respecto. Puede que su ensayo sea sobre algo obvio o trivial, pero también es posible que no lo sea así. Recuerde que, en griego, la palabra *naturaleza* se dice *physis* y, usando ésto como sugerencia, investigue.

EJERCICIO 4. ¿Cuáles de las fórmulas siguientes definen una operación binaria en el conjunto dado?

(i) En $A = \mathbb{N}$, $a \star b := 2a + 3b$.
(ii) En $A = \mathbb{Z}$, $a \star b := 2a - 3b$.
(iii) En $A = \mathbb{N}$, $a \star b := ab - 5$.
(iv) En $A = \mathbb{Q}$, $a \star b := \sqrt{|ab|}$.
(v) En $A = \mathbb{Z}$, $a \star b := \frac{a}{b}$.

EJERCICIO 5. Para cada una de las operaciones binarias siguientes, determine si son o no asociativas:

(i) En $A = \mathbb{Z}$, $a \star b := a - b$.
(ii) En $A = \mathbb{N}$, $a \star b := 2^{a+b}$.
(iii) En $A = \mathbb{R}$, $a \star b := \sqrt{|ab|}$.
(iv) En $A = \mathbb{Z}$, $a \star b := -ab$.
(v) En $A = \mathbb{R}$, $a \star b := a + 2b$.
(vi) En $A = \mathbb{Z}$, $a \star b := a + b - 5$.
(vii) En $A = \mathbb{Q}$, $a \star b := a + b + ab$.

EJERCICIO 6. ¿Cuáles de las operaciones binarias anteriores son conmutativas?

EJERCICIO 7. ¿Cuáles de las operaciones binarias anteriores tienen neutro?

Capítulo 2

Grupos y subgrupos

EN EL CAPÍTULO ANTERIOR VIMOS EL INTERÉS que tiene el que un conjunto G venga equipado con una operación binaria $\bullet$ y también vimos que esta operación binaria puede o no satisfacer ciertas propiedades, que algunas veces hemos tomado por dadas o naturales; desde el punto de vista que estamos adoptando, diremos que el conjunto G tiene una *estructura algebraica* dada por su operación binaria. Dependiendo de las propiedades que satisfaga la operación binaria, se tienen varios tipos de estructuras algebraicas, que van desde las sencillas hasta estructuras más complicadas (que pueden involucrar más de una operación binaria). Nosotros comenzaremos con una estructura que, siendo sencilla, es suficientemente rica para estar presente en varios contextos matemáticos.

Grupos. Un *grupo* es un conjunto no vacío G junto con una operación binaria $\bullet : G \times G \to G$ que satisface las condiciones siguientes:

(i) La operación es *asociativa*, es decir,

$$a \bullet (b \bullet c) = (a \bullet b) \bullet c,$$

para cualesquiera $a, b, c \in G$.

(ii) Existe un *elemento neutro* $e \in G$ que satisface

$$a \bullet e = a = e \bullet a,$$

para todo $a \in G$.

(iii) Para cada elemento $a \in G$ existe otro elemento $a' \in G$ tal que

$$a \bullet a' = e = a' \bullet a.$$

Al elemento a' se le llama un *inverso* del elemento a.

Para enfatizar la importancia de la operación binaria en la definición de un grupo, algunas veces lo denotaremos mediante $(G, \bullet)$.

Ejemplo 1. El grupo de simetrías del cuadrado es el conjunto

$$G = \{e, r, r^2, r^3, \rho, \rho \bullet r, \rho \bullet r^2, \rho \bullet r^3\},$$

donde e es la *acción neutra* que no hace nada, $r = r_{\pi/2}$ y $\rho = \rho_Y$, y con la operación binaria $\alpha \bullet \beta$ dada haciendo β primero y después α, simplificando al final hasta obtener un elemento de G.

Ejemplo 2. Si $G = \mathrm{GL}(2,\mathbb{R})$ es el conjunto de matrices 2×2 con entradas en $\mathbb{R}$ y determinante $\neq 0$, los elementos de $\mathrm{GL}(2,\mathbb{R})$ son las matrices

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

tales que $a, b, c, d \in \mathbb{R}$ y $\det(A) = \det \begin{pmatrix} a & b \\ c & d \end{pmatrix} = ad - bc \neq 0$.

Si $B = \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}$ es otra matriz en $\mathrm{GL}(2,\mathbb{R})$, recordemos que el producto de matrices está definido por:

$$A \bullet B := \begin{pmatrix} a & b \\ c & d \end{pmatrix} \bullet \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} = \begin{pmatrix} aa' + bc' & ab' + bd' \\ ca' + dc' & cb' + dd' \end{pmatrix},$$

y además, como el determinante de un producto de matrices es igual al producto de los determinantes, se tiene que

$$\det(A \bullet B) = \det(A) \cdot \det(B) \neq 0,$$

ya que $\det(A) \neq 0$ y $\det(B) \neq 0$. Entonces, el producto de matrices es una *operación binaria* en $\mathrm{GL}(2,\mathbb{R})$. Mostraremos que $\mathrm{GL}(2,\mathbb{R})$ es un grupo.

(i) Para comenzar, el producto de matrices es asociativo. Si no recuerda cómo se demuestra esto, hágalo como un ejercicio.

(ii) El *neutro* es la matriz identidad

$$I_2 := \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},$$

ya que, si $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}(2,\mathbb{R})$, entonces

$$A \cdot I_2 = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a \cdot 1 + b \cdot 0 & a \cdot 0 + b \cdot 1 \\ c \cdot 1 + d \cdot 0 & c \cdot 0 + d \cdot 1 \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix},$$

por lo que $A \cdot I_2 = A$. Similarmente se muestra que $I_2 \cdot A = A$.

(iii) Si $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, como $\det(A) \neq 0$, entonces A es invertible y su inversa es

$$A^{-1} = \begin{pmatrix} d/\Delta & -b/\Delta \\ -c/\Delta & a/\Delta \end{pmatrix},$$

donde $\Delta = \det(A) = ad - bc \neq 0$, ya que

$$\begin{aligned} A \cdot A^{-1} &= \begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} d/\Delta & -b/\Delta \\ -c/\Delta & a/\Delta \end{pmatrix} \\ &= \begin{pmatrix} (ad-bc)/\Delta & (-ab+ba)/\Delta \\ (cd-dc)/\Delta & (-bc+ad)/\Delta \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \\ &= I_2 \end{aligned}$$

y similarmente se prueba que $A^{-1} \cdot A = I_2$.

Si G es un grupo con operación $\bullet$, diremos que G es *conmutativo* o *abeliano* si para cualesquiera $a, b \in G$ se tiene que

$$a \bullet b = b \bullet a.$$

Note que el grupo $\mathrm{GL}(2, \mathbb{R})$ *no es conmutativo* ya que, por ejemplo, si $A = \begin{pmatrix} 3 & 2 \\ 1 & 4 \end{pmatrix}$ y $B = \begin{pmatrix} 0 & 1 \\ 2 & 5 \end{pmatrix}$, entonces

$$AB = \begin{pmatrix} 3 & 2 \\ 1 & 4 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 2 & 5 \end{pmatrix} = \begin{pmatrix} 4 & 13 \\ 8 & 21 \end{pmatrix}$$

y

$$BA = \begin{pmatrix} 0 & 1 \\ 2 & 5 \end{pmatrix} \begin{pmatrix} 3 & 2 \\ 1 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 4 \\ 11 & 24 \end{pmatrix}$$

por lo que $AB \neq BA$.

Ejemplo 3. En el conjunto $\mathbb{R}$ de números reales se tiene la operación *suma* $+ : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$ que es asociativa, conmutativa y para la cual el elemento cero $0 \in \mathbb{R}$ es neutro: $a + 0 = a$ para $a \in \mathbb{R}$; además todo real $a \in \mathbb{R}$ tiene un *inverso aditivo* $-a \in \mathbb{R}$ tal que $a + (-a) = 0$. Al grupo $(\mathbb{R}, +)$ lo llamaremos el *grupo aditivo de* $\mathbb{R}$.

Ejemplo 4. En $\mathbb{R}$ también se tiene la operación producto $\cdot : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$ que es asociativo y conmutativo y el elemento $1 \in \mathbb{R}$ es *neutro multiplicativo*, i.e., $a \cdot 1 = a$ para todo $a \in \mathbb{R}$. Sin embargo no todo número real tiene *inverso multiplicativo*, a saber el $0 \in \mathbb{R}$ es el único real que no tiene inverso multiplicativo. Así, el conjunto $\mathbb{R}$ no es un grupo con la operación producto de números reales. Pero, quitando al cero, el conjunto $\mathbb{R}^* := \mathbb{R} - \{0\}$, junto con el producto, es un grupo, al que se conoce como el *grupo multiplicativo de números reales*.

Ejemplo 5. El conjunto $\mathbb{Z}$ de números enteros es un grupo con la operación *suma*, al que algunas veces denotaremos por $(\mathbb{Z}, +)$.

Ejemplo 6. En $\mathbb{Z}$ consideremos el subconjunto $\mathbb{Z}^\times = \{1, -1\} \subseteq \mathbb{Z}$, y observemos que con el producto de enteros se tiene que $(\mathbb{Z}^\times, \cdot)$ es un grupo.

Ejemplo 7. Si $n \geq 2$ es un entero, considerando la *divisibilidad por n*, dados dos enteros $a, b \in \mathbb{Z}$ se dice que *a es congruente con b módulo n* si la diferencia $a - b$ es divisible por n, lo cual denotamos por $n|(a-b)$. La definición anterior es una relación de equivalencia en $\mathbb{Z}$ y sus clases de equivalencia se llaman las *clases residuales módulo n*. Se sabe que hay n clases residuales y éstas están dadas por los residuos que quedan al dividir un entero entre n, es decir, si $a \in \mathbb{Z}$, la clase residual módulo n correspondiente a a es el conjunto

$$[a] = \{x \in \mathbb{Z} : \text{al dividir } x \text{ entre } n \text{ el residuo es igual al de dividir } a \text{ entre } n\}.$$

Denotemos por $\mathbb{Z}/n\mathbb{Z}$ al conjunto de clases residuales módulo n. Si $[a] \in \mathbb{Z}/n\mathbb{Z}$, a un elemento $r \in [a]$ lo llamaremos un *representante* de la clase $[a]$. En el conjunto $\mathbb{Z}/n\mathbb{Z}$ se define la *operación* siguiente: dados $[a], [b] \in \mathbb{Z}/n\mathbb{Z}$, escogiendo representantes $a \in [a], b \in [b]$, como $a, b \in \mathbb{Z}$ los podemos sumar en $\mathbb{Z}$ para obtener $a+b \in \mathbb{Z}$ y luego consideramos su clase residual $[a+b] \in \mathbb{Z}/n\mathbb{Z}$. Se define entonces

$$[a] + [b] := [a+b],$$

y se pide al lector que verifique que la *definición* anterior *no depende* de la elección de los representantes de las clases involucradas.

La clase del cero, $[0]$, es neutra para la operación anterior, y si $[a] \in \mathbb{Z}/n\mathbb{Z}$, su inverso es el elemento $[-a]$. La operación es asociativa y conmutativa, por lo que $(\mathbb{Z}/n\mathbb{Z}, +)$ es un grupo abeliano al que llamaremos el *grupo de enteros módulo n*.

El orden de un grupo. Si G es un grupo, su *orden* es el cardinal del conjunto subyacente, $|G|$. Un *grupo finito* es un grupo G cuyo orden es finito, $|G| \in \mathbb{N}$. Un *grupo infinito* es un grupo que no es finito.

Ejemplo 8. El grupo aditivo $(\mathbb{R}, +)$ de los números reales es un grupo infinito. El grupo de simetrías del cuadrado es un grupo finito de orden 8. El grupo aditivo de los enteros módulo n es un grupo finito de orden $|\mathbb{Z}/n\mathbb{Z}| = n$.

Cuando un grupo G es finito, podemos listar sus elementos, digamos $G = \{e = \sigma_1, \sigma_2, \ldots, \sigma_n\}$, y como la operación binaria de G es una función $\bullet : G \times G \to G$, y el producto cartesiano $G \times G$ tiene n^2 elementos, podemos listarlos en una *tabla*, donde en el primer renglón y primera columna se listan los elementos del conjunto G, y si $a, b \in G$, para obtener el elemento $a \bullet b$, localizamos a a en la primera columna y a b en el primer renglón, y el elemento $a \bullet b$ es el elemento dado en la casilla donde se intersectan los lugares de a y b:

$\bullet$	$\cdots$		b	$\cdots$
$\vdots$				
a			$a \bullet b$	
$\vdots$				

Ejemplo 9. Para el grupo aditivo $G = \mathbb{Z}/4\mathbb{Z}$ de los enteros módulo 4, la tabla de su operación, aquí $\bullet$ es la *suma módulo* 4, es:

$+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

Note que, por ejemplo, el inverso de $3 \in \mathbb{Z}/4\mathbb{Z}$ es $-3 = 1$ ya que $3 + 1 = 0$ en $\mathbb{Z}/4\mathbb{Z}$.

Ejemplo 10. Para el grupo de simetrías del cuadrado,

$$G = \{e, r, r^2, r^3, \rho, \rho r, \rho r^2, \rho r^3\},$$

donde e es la *acción neutra* que no hace nada, $r = r_{\pi/2}$ y $\rho = \rho_Y$, el orden del grupo es 8, y se tiene que $\rho^2 = e = r^4$, $r^3\rho = \rho r$ y $r\rho = \rho r^3$ (como se calcula fácilmente de las definiciones de ρ y r), y su tabla de multiplicación está dada por:

$\bullet$	e	r	r^2	r^3	ρ	ρr	ρr^2	ρr^3
e	e	r	r^2	r^3	ρ	ρr	ρr^2	ρr^3
r	r	r^2	r^3	e	ρr^3	ρ	ρr	ρr^2
r^2	r^2	r^3	e	r	ρr^2	ρr^3	ρ	ρr
r^3	r^3	e	r	r^2	ρr	ρr^2	ρr^3	ρ
ρ	ρ	ρr	ρr^2	ρr^3	e	r	r^2	r^3
ρr	ρr	ρr^2	ρr^3	ρ	r^3	e	r	r^2
ρr^2	ρr^2	ρr^3	ρ	ρr	r^2	r^3	e	r
ρr^3	ρr^3	ρ	ρr	ρr^2	r	r^2	r^3	e

La tabla se calcula usando las relaciones dadas al principio. Por ejemplo, $r\rho r = \rho r^3 r = \rho r^4 = \rho$.

Observación. En un grupo finito, dado por una tabla como la anterior, si el grupo es abeliano, la tabla es simétrica con respecto a la diagonal principal. Note también que el inverso de un elemento, digamos a en la columna de la izquierda, se encuentra siguiendo el renglón correspondiente a a hasta localizar el elemento neutro e. El inverso de a es el elemento en el renglón superior arriba de este neutro e.

LEMA 2.1. *Si G es un grupo, entonces:*

(1) *El neutro de G es único.*
(2) *Para cada $\sigma \in G$, su inverso es único.*

Demostración. (1). Si e, e' son dos neutros de G, entonces

$$\begin{aligned} e &= e \bullet e' \quad \text{porque } e' \text{ es neutro} \\ &= e' \quad \text{porque } e \text{ es neutro.} \end{aligned}$$

(2). Si $\sigma \in G$ y si σ', σ'' son dos inversos de σ, entonces

$$\begin{aligned} \sigma' &= \sigma' \bullet e \quad \text{porque } e \text{ es neutro} \\ &= \sigma' \bullet (\sigma \bullet \sigma'') \quad \text{porque } \sigma \bullet \sigma'' = e \\ &= (\sigma' \bullet \sigma) \bullet \sigma'' \\ &= e \bullet \sigma'' \quad \text{porque } \sigma' \bullet \sigma = e \\ &= \sigma''. \end{aligned}$$

□

Notación. Si $\sigma \in G$, denotaremos a su único inverso por σ^{-1}. Si la operación $\bullet$ de G la estamos denotando por $+$, es costumbre denotar al inverso de σ mediante $-\sigma$ y en este caso al neutro de G se le suele denotar por $e = 0$.

Observación. Si $(G, \bullet)$ es un grupo, la ecuación $a \bullet x = b$ tiene una única solución en G, ya que multiplicando la ecuación anterior por a^{-1} a la izquierda, se tiene que: $a^{-1} \bullet (a \bullet x) = a^{-1} \bullet b$, donde

$$a^{-1} \bullet (a \bullet x) = (a^{-1} \bullet a) \bullet x = e \bullet x = x$$

por lo que $x = a^{-1} \bullet b$ es la (única) solución de la ecuación $a \bullet x = b$.

Similarmente, la ecuación $x \bullet a = b$ tiene la (única) solución $x = b \bullet a^{-1}$.

Subgrupos. Si G es un grupo, un *subgrupo* de G es un subconjunto $H \subseteq G$ tal que la operación $\bullet$ de G restringida a H es *cerrada* y H es un grupo con esta operación.

LEMA 2.2. *Sea G un grupo. Un subconjunto $H \subseteq G$ es un subgrupo si y sólo si:*

(1) *Para todo $a, b \in H$ se tiene que $a \bullet b \in H$, i.e., H es cerrado bajo la operación $\bullet$ de G.*
(2) *El neutro $e \in G$ también está en H, i.e., $e \in H$.*
(3) *Si $a \in H$, entonces $a^{-1} \in H$, i.e., H es cerrado bajo inversos.*

Demostración. Si H es un subgrupo, entonces H es un grupo por definición y así, en particular, se satisfacen las propiedades (1), (2) y (3). Recíprocamente, si se satisfacen las propiedades (1), (2), (3), entonces $H \neq \emptyset$ por (2) y como la operación de H es la misma que la de G, entonces la asociatividad en H se hereda de la asociatividad en G y por lo tanto H es un grupo. □

Ejemplo 11. Si $(\mathbb{R}, +)$ es el *grupo aditivo* de los números reales, entonces $\mathbb{Q}$ es un subgrupo. Esto es claro, porque la suma de racionales es racional, el $0 \in \mathbb{R}$ es racional y si $a \in \mathbb{Q}$ entonces $-a \in \mathbb{Q}$.

Similarmente, $\mathbb{Z} \subseteq \mathbb{Q}$ es un subgrupo del grupo aditivo de $\mathbb{Q}$.

Ejemplo 12. Si $(\mathbb{R}^*, \cdot)$ es el *grupo multiplicativo* de los números reales, entonces $\mathbb{Q}^*$ es un subgrupo de $\mathbb{R}^*$ ya que el producto de racionales es racional, el $1 \in \mathbb{R}$ es racional y si $a \in \mathbb{Q}^*$ entonces $a^{-1} \in \mathbb{Q}^*$.

Similarmente, si $\mathbb{Z}^\times := \{1, -1\}$, entonces $\mathbb{Z}^\times \subseteq \mathbb{Q}^*$ es un subgrupo del grupo multiplicativo $\mathbb{Q}^*$.

Notas. Los axiomas que definen un grupo abstracto, esencialmente como lo hicimos en este capítulo, fueron formulados explícitamente, por primera vez, en 1887, por F. G. Frobenius en [33], observando que los teoremas que demostraba sólo dependían de estos axiomas y no hacía falta el lenguaje de los grupos de permutaciones vistos como subgrupos del grupo simétrico que usaban sus predecesores, en particular Cauchy, Jordan y Sylow. En su artículo, Frobenius cita a Kronecker [47] como antecedente para la formulación de los axiomas de grupo y en el artículo de Kronecker encontramos la definición de operación binaria, esencialmente como vimos en el capítulo anterior y Kronecker lista una serie de propiedades de estas operaciones binarias que equivalen a los axiomas que satisface un grupo abeliano finito.

De hecho, la afirmación principal del párrafo anterior debe ser modulada: En 1854, Cayley [29] formula lo que podría considerarse la primera definición de un grupo abstracto finito, que traducida dice:

> «Un conjunto de símbolos $1, \alpha, \beta, \ldots$, todos los cuales son diferentes y que satisfacen que el producto de cualesquiera dos de ellos (no importando el orden) o el producto de uno cualquiera de ellos por sí mismo, pertenece al conjunto, se dice que es un *grupo*.»

Sin embargo, aparentemente, los matemáticos de esa época no estaban preparados o interesados para una tal abstracción, siendo grupos concretos, como los de permutaciones, los que les importaban para investigación, de tal manera que la definición abstracta de Cayley no trascendió.

En el artículo [47] citado por Frobenius, Kronecker define una operación binaria en un conjunto finito y requiere que se satisfagan ciertas condiciones que equivalen a los axiomas de un grupo abeliano finito:

«Sean $\theta', \theta'', \theta''', \ldots$ un número finito de elementos tales que con cualquiera dos de ellos está asociado un tercer elemento por medio de un procedimiento definido. Así, si f denota este procedimiento y si θ' y θ'' son dos elementos (posiblemente iguales), entonces existe un θ''' igual a $f(\theta', \theta'')$. Más aún, $f(\theta', \theta'') = f(\theta'', \theta')$, $f(\theta, f(\theta', \theta''')) = f(f(\theta, \theta'), \theta''')$ y si θ'' es diferente de θ''', entonces $f(\theta, \theta')$ es diferente de $f(\theta, \theta''')$. Asumiendo ésto, podemos reemplazar la operación $f(\theta', \theta'')$ por la multiplicación $\theta' \cdot \theta''$ si en lugar de la igualdad usamos la equivalencia $\sim$ definiendo $\theta' \cdot \theta'' \sim \theta'''$ por medio de la ecuación $f(\theta', \theta'') = \theta'''$.»

Kronecker observa que el punto de vista adoptado permite aplicaciones en varios contextos, particularmente en la teoría de números, haciendo innecesario repetir el mismo argumento en casos diferentes y, además, la presentación gana en simpleza haciendo transparentes los aspectos verdaderamente esenciales de la teoría.

También debe mencionarse que, en un artículo de 1882, sobre formas cuadráticas, H. Weber [55] formula (*redescubre*) la definición de grupo abstracto finito como:

«Un sistema G de un número finito h de elementos arbitrarios θ_1, $\theta_2, \ldots, \theta_h$ se dice que es un *grupo* de *grado* h si satisface las condiciones siguientes:

I. Se tiene una regla, llamada *composición* o *multiplicación*, por medio de la cual de cualesquiera dos elementos del mismo sistema se deriva un nuevo elemento del mismo sistema. En símbolos $\theta_r \theta_s = \theta_t$.

II. Se tiene que:

$$(\theta_r \theta_s)\theta_t = \theta_r(\theta_s \theta_t) = \theta_r \theta_s \theta_t.$$

III. De $\theta\theta_r = \theta\theta_s$ o de $\theta_r\theta = \theta_s\theta$, se sigue que $\theta_r = \theta_s$.»

Las definiciones anteriores, válidas sólo para grupos finitos, reflejan, de alguna manera, dos de las fuentes que dieron origen a la teoría de grupos, a saber, los grupos de permutaciones (de raíces de polinomios, como en Galois [40] o Lagrange [48], o de conjuntos finitos arbitrarios como en Cauchy [27]) y los grupos abelianos finitos provenientes de la teoría de números, como en Kronecker [47] o Weber [55]. Grupos infinitos, provenientes de la geometría como grupos de transformaciones (continuas o discontinuas) fueron incluidos, por primera vez, en una definición de grupo abstracto, en 1882, por W. Dieck en [31] en términos de lo que hoy llamaríamos *generadores* y *relaciones*; el artículo de W. Dieck comienza con un epígrafe citando a Cayley [30], enfatizando que:

«Un grupo está definido por medio de las leyes de combinación de sus símbolos.»

Al incluir, en su definición, grupos infinitos, Dieck fue el primero en requerir explícitamente la existencia de inversos:

> «Requerimos para nuestras consideraciones que un grupo que contenga a la operación T_k también debe contener a la operación T_k^{-1}.»

Este es el contexto histórico que permite la formulación de los axiomas de grupo (finito o infinito) por Frobenius [33] en 1887 y que mencionamos al inicio de esta nota.

EJERCICIO 1. Si G es el grupo de simetrías del cuadrado, ¿es G abeliano? ¿Cuál es su orden? Liste todos los subgrupos de este grupo. ¿Cuál es el orden de sus elementos? Haga lo mismo para un triángulo equilátero, un pentágono y un hexágono regulares.

EJERCICIO 2. Sea $\mu_n = \{z \in \mathbb{C} \ : \ z^n = 1\}$ el conjunto de todas las raíces n-ésimas de 1. Con el producto de números complejos muestre que μ_n es un grupo abeliano. ¿Cuál es su orden?

EJERCICIO 3. Sea $\mathrm{GL}(2, \mathbb{F}_2)$ el conjunto de todas las matrices 2×2 con entradas en $\mathbb{F}_2 = \{\overline{0}, \overline{1}\}$ (los enteros módulo 2) y con determinante $\neq \overline{0}$. Calcule el orden de este grupo.

EJERCICIO 4. Si $\mathrm{SL}(2, \mathbb{F}_2)$ es el subconjunto de $\mathrm{GL}(2, \mathbb{F}_2)$ formado por las matrices con determinante $= \overline{1}$, muestre que $\mathrm{SL}(2, \mathbb{F}_2)$ es un subgrupo de $\mathrm{GL}(2, \mathbb{F}_2)$. ¿Cuál es el orden de este subgrupo?

EJERCICIO 5. Sea $n \geq 1$ un entero. Muestre que el conjunto

$$n\mathbb{Z} = \{nx \ : \ x \in \mathbb{Z}\}$$

de múltiplos de n, es un subgrupo de $\mathbb{Z}$.

EJERCICIO 6. Si m, n son enteros tales que $m|n$, demuestre que $n\mathbb{Z}$ es un subgrupo de $m\mathbb{Z}$.

EJERCICIO 7. Si G es un grupo, el *centro de* G es el conjunto

$$Z(G) := \{g \in G \ : \ g \bullet x = x \bullet g \quad \text{para todo } x \in G\},$$

(el conjunto de los elementos de G que conmutan con todos los elementos de G).

(i) Demuestre que $Z(G)$ es un subgrupo de G.
(ii) Demuestre que $Z(G)$ es abeliano.
(iii) ¿Qué pasa si G es abeliano?

EJERCICIO 8. Si G es un grupo y $\alpha \in G$, el *centralizador* de α en G es el conjunto

$$C_G(\alpha) := \{g \in G \ : \ g \bullet \alpha = \alpha \bullet g\}$$

de elementos de G que conmutan con α. Demuestre que $C_G(\alpha)$ es un subgrupo de G.

EJERCICIO 9. Si G es un grupo que tiene un único elemento g de orden 2, demuestre que $C_G(g) = G$.

EJERCICIO 10. Verifique que la definición de la suma en $\mathbb{Z}/n\mathbb{Z}$ es, en efecto, una buena definición, es decir, que no depende de la elección de los representantes de las clases involucradas: si $a, a' \in [a]$ y $b, b' \in [b]$, demuestre que $[a + b] = [a' + b']$.

EJERCICIO 11. Sea G un grupo y $H \subseteq G$ un subconjunto no vacío. Demuestre que H es un subgrupo si y sólo si $a \bullet b^{-1} \in H$ para todo $a, b \in H$.

EJERCICIO 12. Si G es cualquier grupo y si $g \in G$, demuestre que $(g^{-1})^{-1} = g$.

EJERCICIO 13. Si G es un grupo y si $g, h \in G$, demuestre que $(g \bullet h)^{-1} = h^{-1} \bullet g^{-1}$.

EJERCICIO 14. Sean G un grupo y $H \subseteq G$ un subconjunto *finito* no vacío tal que H es cerrado bajo la operación de G (es decir, $a, b \in H \Rightarrow a \bullet b \in H$). Demuestre que H es un subgrupo de G.

Capítulo 3

Grupos cíclicos

SI $(G, \bullet)$ ES UN GRUPO, dado un elemento $\sigma \in G$ se definen sus *potencias enteras* σ^k con $k \in \mathbb{Z}$ mediante las igualdades siguientes:

(i) Si $k = 0$ se define $\sigma^0 := e$.
(ii) Si $k \geq 1$, se definen

$$\begin{aligned} \sigma^1 &:= \sigma \\ \sigma^2 &:= \sigma \bullet \sigma \\ \sigma^3 &:= \sigma^2 \bullet \sigma \\ &\vdots \\ \sigma^{k+1} &:= \sigma^k \bullet \sigma \end{aligned}$$

(decimos que ésta es una definición *recursiva* o inductiva).
(iii) Si $-k < 0$, como $k > 0$, se define

$$\sigma^{-k} := (\sigma^{-1})^k$$

donde σ^{-1} es la inversa de σ y la potencia de $(\sigma^{-1})^k$ es con exponente positivo, la cual ya definimos en el paso (ii).

Es un ejercicio el probar que se satisface la *ley de los exponentes*:

$$\sigma^m \bullet \sigma^n = \sigma^{m+n},$$

para cualesquiera $m, n \in \mathbb{Z}$.

Notación. Si $(G, \bullet)$ es un grupo, y si por alguna razón denotamos a su operación por $+$, entonces es costumbre denotar a su elemento neutro por 0 y al inverso de $\sigma \in G$ por $-\sigma$. También, las *potencias* con exponente k se denotan aditivamente, i.e., σ^k se denota $k\sigma$. Por ejemplo, la igualdad $\sigma^0 = e$ se denota $0\sigma = 0$. También, en muchas ocasiones, si el grupo G es un grupo arbitrario, la operación $a \bullet b$ en G la denotaremos mediante yuxtaposición, es decir, mediante ab, obviando al símbolo $\bullet$

LEMA 3.1. *Si G es un grupo y $\sigma \in G$ es cualquier elemento, el conjunto*

$$\langle \sigma \rangle := \langle \sigma^n \ : \ n \in \mathbb{Z} \rangle$$

es un subgrupo de G.

Demostración. Por definición $\sigma^0 = e$ y así $e \in \langle \sigma \rangle$. Observe ahora que $\langle \sigma \rangle$ es cerrado bajo productos, ya que si $\sigma^m, \sigma^n \in \langle \sigma \rangle$, entonces $\sigma^m \sigma^n = \sigma^{m+n}$ es un elemento de $\langle \sigma \rangle$. También, si $\sigma^m \in \langle \sigma \rangle$, entonces $\sigma^{-m} \in \langle \sigma \rangle$ satisface que

$$\sigma^{-m} \sigma^m = \sigma^0 = e$$

por lo que el inverso de σ^m es σ^{-m}. □

El grupo $\langle \sigma \rangle$ del lema anterior se llama el *subgrupo cíclico generado* por σ. Un grupo G se dice que es un *grupo cíclico* si existe un elemento $\sigma \in G$ tal que

$$G = \langle \sigma \rangle.$$

Al elemento σ se le llama un *generador* de G.

Ejemplo 1. El grupo aditivo de los enteros $\mathbb{Z}$ es cíclico, generado por el 1.

Ejemplo 2. El grupo aditivo de los racionales $\mathbb{Q}$ no es cíclico. (Ejercicio 10).

Ejemplo 3. Si $n \geq 1$ es un entero, el grupo aditivo de los enteros módulo n,

$$\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{n-1}\}$$

es cíclico, generado por el $\overline{1}$.

Los grupos cíclicos son, de alguna manera, muy sencillos, por ejemplo, son abelianos:

PROPOSICIÓN 3.2. *Todo grupo cíclico es abeliano.*

Demostración. Si G es cíclico, digamos $G = \langle \sigma \rangle$, para algún $\sigma \in G$. Entonces, todos los elementos de G son de la forma σ^k, para k un entero. Así, si $a, b \in G$ son dos elementos arbitrarios, entonces a y b son de la forma $a = \sigma^m$ y $b = \sigma^n$, por lo que

$$ab = \sigma^m \sigma^n = \sigma^{m+n} = \sigma^{n+m} = \sigma^n \sigma^m = ba$$

(usamos que $m + n = n + m$ en $\mathbb{Z}$). □

Los subgrupos de un grupo cíclico también son sencillos:

PROPOSICIÓN 3.3. *Los subgrupos de un grupo cíclico también son cíclicos.*

Demostración. Supongamos que $G = \langle \sigma \rangle$, para algún $\sigma \in G$, y sea H un subgrupo de G. Si $H = \{e\}$, entonces ciertamente H es cíclico generado por e, i.e., $H = \{e\} = \langle e \rangle$. Si $H \neq \{e\}$, entonces H contiene un elemento de la forma σ^k con $k \neq 0$. Como H es subgrupo entonces también contiene al elemento $(\sigma^k)^{-1} = \sigma^{-k}$. Como $k \neq 0$, por tricotomía $k > 0$ ó $-k > 0$. Hemos así mostrado que H contiene un elemento de la forma σ^m con $m > 0$. Sea $n > 0$ el menor entero positivo tal que $\sigma^n \in H$. Mostraremos que $a = \sigma^n$ genera a H, i.e., que $H = \langle a \rangle = \langle \sigma^n \rangle$ y para esto debemos probar que todo elemento $h \in H$ es una potencia de a. En efecto, como $h \in H \subseteq G$, entonces $h \in G$ y por lo tanto h es de la forma $h = \sigma^t$ para algún $t \in \mathbb{Z}$. Dividiendo el entero t entre el entero n dado por $a = \sigma^n$, se tiene que

$$t = nq + r, \qquad \text{con } q, r \in \mathbb{Z} \text{ y } 0 \leq r < n$$

(por el algoritmo de la división en $\mathbb{Z}$). Se sigue que

$$\sigma^t = \sigma^{nq+r} = \sigma^{nq}\sigma^r = (\sigma^n)^q\sigma^r = a^q\sigma^r$$

y por lo tanto, despejando, $\sigma^r = a^{-q}\sigma^t$. Ahora, como $a, \sigma^t \in H$ y H es un subgrupo, entonces $a^{-q}\sigma^t \in H$, i.e.,

$$\sigma^r \in H \quad \text{con } 0 \leq r < n \tag{1}$$

y como σ^n es la menor potencia positiva de σ en H, entonces (1) implica que $r = 0$, es decir,

$$e = \sigma^0 = a^{-q}\sigma^t$$

y despejando $\sigma^t = a^q \in \langle a \rangle$. Se sigue que $H = \langle a \rangle$. □

Ejemplo 4. Por el primer ejemplo, $\mathbb{Z}$ es un grupo cíclico, generado por el 1. Entonces, la proposición anterior nos dice que todos los subgrupos de $\mathbb{Z}$ son cíclicos, generados por una *potencia* de 1, i.e., por un elemento de la forma $n \cdot 1 = n$. Por lo tanto los subgrupos de $\mathbb{Z}$ son de la forma

$$H = n\mathbb{Z} = \{nk \ : \ k \in \mathbb{Z}\} = \text{múltiplos enteros de } n.$$

Grupos cíclicos infinitos. El ejemplo $\mathbb{Z}$ es un grupo cíclico de orden infinito y todos sus subgrupos, exceptuando el subgrupo trivial $\{0\}$ también son infinitos. Podemos hacernos la pregunta ¿cómo será otro grupo cíclico infinito? Supongamos que G es un grupo cíclico infinito generado por g, i.e., $G = \langle g \rangle$. Entonces, los elementos de G son de la forma g^ℓ con $\ell \in \mathbb{Z}$. Comenzamos mostrando que si $m \neq n$ son dos enteros diferentes, entonces $g^m \neq g^n$. En efecto, como $m \neq n$, podemos suponer, sin perder generalidad, que $m > n$. Ahora, si sucediera que $g^m = g^n$, con $m > n$, entonces $m - n > 0$ y multiplicando la igualdad $g^m = g^n$ por g^{-n} se obtiene:

$$g^{m-n} = g^m g^{-n} = g^n g^{-n} = g^0 = e,$$

i.e., $g^{m-n} = e$ con $m-n > 0$. Sea $k > 0$ el menor entero positivo tal que $g^k = e$. (Note la similaridad con la idea de la demostración de que los subgrupos de un grupo cíclico también son cíclicos). Mostraremos que $G = \{e, g, g^2, \ldots, g^{k-1}\}$, i.e., G sería finito, lo cual es una contradicción. Para mostrar que $G = \{e, g, g^2, \ldots, g^{k-1}\}$, mostraremos que cualquier elemento de G está en el conjunto de la derecha. En efecto, si $g^m \in G$ es cualquier elemento, dividiendo m entre el entero k anterior, obtenemos

$$m = kq + r \quad \text{con } 0 \leq r < k$$

y por lo tanto

$$g^m = g^{kq+r} = (g^k)^q g^r = e^q g^r = g^r$$

es decir, la potencia g^m es igual a g^r con $0 \leq r < k$. Es decir, cualquier elemento de G es uno de los elementos: $e = g^0, g, g^2, \ldots, g^{k-1}$, como se quería. Como esto contradice el hecho de que G es infinito, se sigue que todas las potencias g^m son diferentes. Hemos probado así el teorema siguiente:

TEOREMA 3.4. *Si G es un grupo cíclico infinito, digamos generado por g, entonces todas las potencias g^m son distintas.*

□

Grupos cíclicos finitos. El ejemplo 3 es un grupo cíclico finito, a saber $\mathbb{Z}/n\mathbb{Z}$ el grupo aditivo de los enteros módulo n. La pregunta que nos hacemos ahora es: ¿cómo será otro grupo cíclico finito G? Para comenzar, si $G = \langle g \rangle$ es finito de orden n, no puede suceder que todas las potencias de g sean diferentes, porque al pertenecer éstas a G, entonces G sería infinito. Se sigue que existen enteros $i \neq j$ tales que $g^i = g^j$. Por tricotomía y sin perder generalidad, podemos suponer que $i > j$ y así la igualdad $g^i = g^j$ implica que

$$g^{i-j} = g^i g^{-j} = g^j g^{-j} = g^0 = e,$$

i.e., existe un entero positivo ℓ tal que $g^\ell = e$. Sea k el menor entero positivo tal que $g^k = e$. Entonces,

$$\{e = g^0, g, g^2, g^3, \ldots, g^{k-1}\} \subseteq G.$$

Probaremos que se tiene la igualdad en la inclusión anterior, i.e., que $k = n$. Para comenzar, la inclusión de arriba nos dice que $k \leq n$. Para probar la otra desigualdad, recordemos que los elementos de G son de la forma g^ℓ con $\ell \in \mathbb{Z}$. Dividiendo ℓ entre k se obtiene $\ell = kq + r$, con $0 \leq r < k$ y, como en el argumento para el caso cíclico infinito, se tiene que:

$$g^\ell = g^{kq+r} = g^{kq} g^r = (g^k)^q g^r = e^q g^r = g^r,$$

y así $g^\ell = g^r$, i.e., todas las potencias g^ℓ son algunas de las g^r con $0 \leq r < k$ y por lo tanto $g^\ell \in \{e = g^0, g, g^2, g^3, \ldots, g^{k-1}\}$, por lo que

$$G = \{e = g^0, g, g^2, g^3, \ldots, g^{k-1}\}$$

y $n = k$, como se quería. Hemos así probado la primera parte de:

TEOREMA 3.5. (1) *Si G es un grupo cíclico finito, entonces los elementos de G son potencias positivas de g, desde $g^0 = e$ hasta g^{k-1}, donde $k = |G|$ es el orden del grupo y es el menor entero positivo que anula a g. Así*

$$G = \{e = g^0, g, g^2, g^3, \ldots, g^{k-1}\}.$$

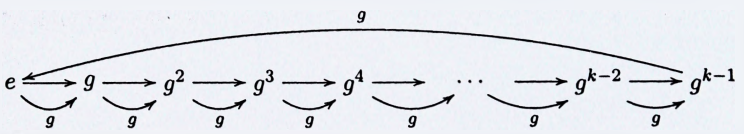
(2) *También, si $\ell \geq 1$ es un entero tal que $g^\ell = e$, entonces $k|\ell$.*

Demostración. Sólo resta probar la parte (2). Para esto, dividiendo ℓ entre k tenemos $\ell = kq + r$, con $0 \leq r < k$ y así

$$e = g^\ell = g^{kq+r} = (g^k)^q g^r = eg^r = g^r,$$

y como k es el menor exponente positivo que anula a g, la igualdad anterior implica que $r = 0$ y por lo tanto $k|\ell$. □

Note la ventaja de lo anterior, ya que en la definición de grupo cíclico incluíamos potencias positivas y negativas, y lo que acabamos de probar nos dice que, en el caso finito, basta tomar potencias positivas del generador hasta llegar al orden k del grupo (ya que $g^k = e = g^0$). Podemos ilustrar la forma en que se operan los elementos del grupo cíclico $G = \langle g \rangle$ con el diagrama siguiente, donde las flechas curvas indican multiplicación por g, en particular, $gg^{k-1} = g^k = e$. Note lo *cíclico* del diagrama, i.e., después de llegar a g^{k-1}, se *repiten* los valores:



¿Cómo serán los subgrupos de un grupo cíclico finito? Por la proposición 3.3 anterior, por supuesto que también son cíclicos. Las preguntas son entonces: (i) ¿qué orden tienen? y (ii) ¿cómo son sus generadores? Las respuestas a estas preguntas son:

PROPOSICIÓN 3.6. *Sea G un grupo cíclico de orden n y generado por un elemento g. Sea $\sigma \in G$ dado por $\sigma = g^k$. Entonces, σ genera un subgrupo cíclico de G de orden n/d, donde $d = \text{mcd}(n, k)$.*

Demostración. Sólo debemos mostrar que el orden de $\langle \sigma \rangle$ es n/d. Ahora, como $\sigma = g^k$, entonces, por el argumento usado en el teorema anterior, el orden del subgrupo $\langle \sigma \rangle$ es el menor exponente positivo de $\sigma = g^k$ que se anula, i.e., es el menor entero $\ell \geq 1$ tal que

$$(g^k)^\ell = e.$$

Ahora, por el mismo argumento del teorema anterior, como $G = \langle g \rangle$ es de orden n, entonces n es el menor entero positivo tal que g se anula al elevarse a ese exponente, entonces la igualdad $e = (g^k)^\ell = g^{k\ell}$ implica (por la parte 2 del teorema anterior) que n divide a $k\ell$. Ahora, si $d = \text{mcd}(n, k)$ entonces $d|n$ y $d|k$. Escribiendo $n = d(n/d)$ y $k = d(k/d)$, entonces n/d y k/d son coprimos y como $n|k\ell$, entonces $(n/d)|(k/d)\ell$ con $\text{mcd}(n/d, k/d) = 1$, por lo que n/d debe dividir al factor ℓ y consecuentemente $(n/d) \leq \ell$. Ahora, como

$$(g^k)^{n/d} = (g^n)^{k/d} = e,$$

y como $(n/d) \leq \ell$ y ℓ es el menor exponente que anula a g^k, entonces se debe tener que $\ell = n/d$, como se quería. □

Observe que, si $G = \langle g \rangle$ es de orden n y $k \geq 1$ es *coprimo* con n, i.e., $\text{mcd}(n, k) = 1$, entonces el elemento g^k genera un subgrupo de G de orden $\frac{n}{1} = n$, i.e., de orden n, y por lo tanto este subgrupo de G es todo G. Hemos así probado:

COROLARIO 3.7. *Sea G un grupo cíclico de orden n y generado por un elemento g. Entonces, los otros generadores de G son de la forma g^k, con $k \geq 1$ coprimo con n.*

□

El orden de un elemento. Si G es un grupo y $\sigma \in G$ es cualquier elemento, diremos que σ tiene *orden infinito* si para cualquier entero $k \geq 1$ se tiene que $\sigma^k \neq e$. Es decir, si ninguna potencia con k positiva se *muere*. Si existe un entero $k \geq 1$ tal que $\sigma^k = e$, al menor de esos enteros positivos se le llama el *orden de* σ. Por ejemplo, el orden de e es 1; y e es el único elemento de orden 1 en G. Si $\sigma \neq e$, el orden de σ es k si $\sigma^k = e$ y $\sigma^j \neq e$ para todo $1 \leq j < k$.

Ejemplo 5. Si G es el grupo de simetrías del cuadrado,

$$G = \{e, r, r^2, r^3, \rho, \rho r, \rho r^2, \rho r^3\}$$

el elemento e es de orden 1. El elemento r es de orden 4, el elemento r^2 es de orden 2, el elemento r^3 es de orden 4, el elemento ρ es de orden 2, el elemento ρr es de orden 2 ya que

$$(\rho r)(\rho r) = \rho(r\rho)r = \rho(\rho r^3)r = \rho^2 r^4 = e.$$

Observación. Si G es un grupo finito, de orden digamos n, entonces cualquier elemento $a \in G$ tiene orden $\leq n$, ya que de lo contrario, por ejemplo si a tiene orden $> n$, entonces en G estarían los elementos distintos $a, a^2, a^3, \ldots, a^k$ con $k > n$, una contradicción. Se sigue que todos los elementos de G tienen orden finito $\leq n$. ¿Qué sucede cuando G tiene un elemento de orden $n = |G|$?

PROPOSICIÓN 3.8. *Si G es un grupo finito de orden n, entonces G es cíclico, generado por $g \in G$, si y sólo si g es un elemento de orden $n = |G|$.*

Demostración. Si $n = 1$, entonces $G = \{e\}$ y no hay nada que probar. Supongamos entonces que $n > 1$ y que G es cíclico de orden n, generado por $g \in G$; entonces

$$G = \{g, g^2, g^3, \ldots, g^{n-1}, g^n = e\}$$

y como estos son los n elementos de G, entonces se debe tener que $g^k \neq e$ para toda $1 \leq k < n$ y por lo tanto el generador g de G tiene orden n.

Recíprocamente, si existe un elemento $\sigma \in G$ de orden n, entonces se tiene el subgrupo

$$\langle \sigma \rangle = \{\sigma, \sigma^2, \sigma^3, \ldots, \sigma^{n-1}, \sigma^n = e\} \subseteq G$$

de G con exactamente n elementos, i.e., se tiene el subgrupo

$$\langle \sigma \rangle \subseteq G$$

de orden $|\langle \sigma \rangle| = n$ y por lo tanto debe ser igual a G, i.e., $G = \langle \sigma \rangle$, por lo que G es cíclico, generado por σ. □

Notas. El teorema 3.4 esencialmente nos dice que hay una biyección entre un grupo cíclico infinito arbitrario y el grupo aditivo $\mathbb{Z}$, y la parte 1 del teorema 3.5 nos dice que hay una biyección entre un grupo cíclico finito de orden k y el grupo de enteros módulo k, $\mathbb{Z}/k\mathbb{Z}$. De hecho, estas biyecciones son algo más y, en el capítulo 6, ejemplos 10 y 11, veremos que esencialmente sólo hay un grupo cíclico infinito, $\mathbb{Z}$, y sólo hay un grupo cíclico finito de orden k, a saber $\mathbb{Z}/k\mathbb{Z}$.

EJERCICIO 1. Si G es el grupo de simetrías del cuadrado, ¿es G cíclico? Liste todos los subgrupos cíclicos de G. Haga lo mismo para un triángulo equilátero, un pentágono y un hexágono regulares.

EJERCICIO 2. Sea $\mu_n = \{z \in \mathbb{C} : z^n = 1\}$ el grupo de las raíces n-ésimas de 1 (vea el ejercicio 2 del capítulo 2). Demuestre que μ_n es cíclico. Liste todos sus generadores.

EJERCICIO 3. Sea $\mathrm{GL}(2, \mathbb{F}_2)$ el grupo de matrices 2×2 con entradas en $\mathbb{F}_2 = \{\bar{0}, \bar{1}\}$ con determinante $\neq \bar{0}$ (vea el ejercicio 3 del capítulo 2). ¿Es $\mathrm{GL}(2, \mathbb{F}_2)$ cíclico?

EJERCICIO 4. Si $H = m\mathbb{Z}$ y $K = n\mathbb{Z}$ son subgrupos de $\mathbb{Z}$ (vea el ejemplo 4), ¿quién es $m\mathbb{Z} \cap n\mathbb{Z}$?

EJERCICIO 5. Si G es un grupo y H, K son subgrupos de G, demuestre que $H \cap K$ es un subgrupo de G.

EJERCICIO 6. En general, si $\mathcal{F} = \{H_\alpha : \alpha \in \Gamma\}$ es una familia (no vacía) de subgrupos de G, demuestre que $\bigcap_{\alpha \in \Gamma} H_\alpha$ es un subgrupo de G.

EJERCICIO 7. Sean G un grupo y $S \subseteq G$ un subconjunto (no vacío). Sea $\mathcal{F}$ la familia de subgrupos de G que contienen al conjunto S.

(i) Observe que $G \in \mathcal{F}$ y así $\mathcal{F}$ no es vacía. Por el ejercicio anterior, la intersección de la familia $\mathcal{F}$ es un subgrupo de G al que se llama el *subgrupo generado* por S y se denota $\langle S \rangle$. Los elementos de S se dice que son los *generadores* del grupo $\langle S \rangle$.

(ii) Muestre que $S \subseteq \langle S \rangle$.

(iii) Si $H \subseteq G$ es cualquier subgrupo que contiene a S, demuestre que $\langle S \rangle \subseteq H$. En este sentido, $\langle S \rangle$ es el *menor subgrupo de G que contiene a S*.

(iv) Si $S = \{g\} \subseteq G$, demuestre que $\langle S \rangle = \langle \{g\} \rangle = \langle g \rangle$ es el subgrupo cíclico generado por g.

(v) En general, si $S = \{g_1, \ldots, g_k\}$, denotaremos al grupo $\langle S \rangle$ por $\langle g_1, \ldots, g_k \rangle$.

EJERCICIO 8. Si G es un grupo que no tiene subgrupos no triviales, demuestre que G es finito de orden primo.

EJERCICIO 9. Si G es un grupo finito de orden par, demuestre que existe un elemento $g \in G$ de orden 2.

EJERCICIO 10. Demuestre que el grupo $(\mathbb{Q}, +)$ no es cíclico.

EJERCICIO 11. Si $G = \langle g \rangle$ es cíclico de orden n, demuestre que para todo $i, j = 0, 1, \ldots, n-1$, $g^i g^j = g^k$ si y sólo si $i + j \equiv k \pmod{n}$.

EJERCICIO 12. Si $G = \langle g \rangle$ es cíclico de orden p^n, para p un primo, demuestre que

$$1 \subseteq \langle g^{p^{n-1}} \rangle \subseteq \langle g^{p^{n-2}} \rangle \subseteq \cdots \subseteq \langle g^p \rangle \subseteq G$$

son todos los subgrupos de G.

Capítulo 4

Grupos de permutaciones

Si $n \geq 1$ es un entero, denotemos con $\mathbb{I}_n := \{1, 2, \ldots, n\}$ al subconjunto de los números naturales del 1 al n. Diremos que $\mathbb{I}_n$ es un *intervalo* de naturales. Una función biyectiva $\sigma : \mathbb{I}_n \to \mathbb{I}_n$ se llamará una *permutación* de $\mathbb{I}_n$. Esta función la podemos representar mediante:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ \sigma(1) & \sigma(2) & \sigma(3) & \cdots & \sigma(n) \end{pmatrix}$$

donde debajo de cada natural $x \in \mathbb{I}_n$ hemos colocado su valor o imagen $\sigma(x) \in \mathbb{I}_n$.

Ejemplo 1. Si $n = 4$, se tienen las permutaciones siguientes:

$$e = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}, \quad \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 4 & 3 \end{pmatrix},$$

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{pmatrix}, \quad \vartheta = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}.$$

Note que una permutación α de $\mathbb{I}_4$ *cambia de lugar* los enteros $1, 2, 3, 4$. Es decir, en la notación de arriba, los enteros que aparecen en el renglón inferior son *todos* los números enteros del 1 al 4, y aparecen *una sóla vez*. Lo anterior es sólo una reformulación del hecho de que la permutación α es una función *biyectiva*, i.e., es *inyectiva* y *suprayectiva*.

Sea S_n el conjunto de todas las permutaciones de $\mathbb{I}_n$. Si $\sigma, \tau \in S_n$, escribiendo estas funciones con su dominio y codominio:

$$\sigma : \mathbb{I}_n \to \mathbb{I}_n \qquad \text{y} \qquad \tau : \mathbb{I}_n \to \mathbb{I}_n$$

es claro que las podemos *componer* para obtener la función:

$$\tau \circ \sigma : \mathbb{I}_n \to \mathbb{I}_n$$

dada por $(\tau \circ \sigma)(x) := \tau(\sigma(x))$. Como τ y σ son biyectivas, la composición $\tau \circ \sigma$ también es biyectiva y así

$$\tau \circ \sigma \in S_n,$$

es decir, la composición de funciones es una operación binaria en S_n. Recordemos ahora que la composición de funciones es *asociativa* en general. Se sigue que la operación binaria $\circ$ de S_n es asociativa. También, si

$$e = \mathrm{id}_n : \mathbb{I}_n \to \mathbb{I}_n$$

es la *función identidad* dada por $\mathrm{id}_n(x) := x$, para cualquier $x \in \mathbb{I}_n$, entonces id_n es una función biyectiva y por lo tanto $\mathrm{id}_n \in S_n$. Observe ahora que, para cualquier permutación $\sigma \in S_n$, se tiene que $\mathrm{id}_n \circ \sigma = \sigma$ ya que

$$(\mathrm{id}_n \circ \sigma)(x) = \mathrm{id}_n(\sigma(x)) = \sigma(x)$$

y similarmente se muestra que $\sigma \circ \mathrm{id}_n = \sigma$. Finalmente, si $\sigma \in S_n$, como σ es biyectiva, entonces tiene una *función inversa* $\sigma^{-1} : \mathbb{I}_n \to \mathbb{I}_n$ dada por

$$\sigma^{-1}(y) = x \Leftrightarrow \sigma(x) = y.$$

La función $\sigma^{-1} \in S_n$ satisface que

$$\sigma \circ \sigma^{-1} = \mathrm{id}_n \qquad \text{y} \qquad \sigma^{-1} \circ \sigma = \mathrm{id}_n,$$

es decir, σ^{-1} es la *inversa* de σ en S_n. Hemos así mostrado que:

PROPOSICIÓN 4.1. *El conjunto S_n de funciones biyectivas de $\mathbb{I}_n$ en $\mathbb{I}_n$ es un grupo, con la operación dada por la composición de funciones.*

□

El grupo $(S_n, \circ)$ se llama el *grupo simétrico en n letras*. Es conocido que hay $n!$ funciones biyectivas de $\mathbb{I}_n$ en $\mathbb{I}_n$ y así S_n es un grupo finito de orden $|S_n| = n! = 1 \cdot 2 \cdot 3 \cdots n$.

Ejemplo 2. Si $n = 4$, el grupo S_4 tiene orden $|S_4| = 4! = 1 \cdot 2 \cdot 3 \cdot 4 = 24$. La composición de dos permutaciones en S_4 es fácil, usando la notación introducida previamente, para τ y ϑ como en el ejemplo 1,

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{pmatrix} \quad \text{y} \quad \vartheta = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix},$$

se tiene que

$$\begin{aligned} \tau \circ \vartheta &= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \\ 2 & 4 & 3 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix}, \end{aligned}$$

donde, en la segunda igualdad se calculó primero la acción de ϑ y luego la acción de τ; note que añadimos un renglón extra para hacer explícitos los cálculos, por ejemplo,

como $\vartheta(2) = 3$, entonces $\tau(\vartheta(2)) = \tau(3) = 4$. La última igualdad elimina el renglón extra y escribe en la notación usual al resultado de componer las permutaciones ϑ y τ.

Observe también que es fácil ver la inversa de una permutación, por ejemplo, si

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{pmatrix}$$

la inversa se calcula leyendo el renglón inferior primero para que las imágenes sean los valores en el primer rengón, y así se obtiene:

$$\tau^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 2 & 3 \end{pmatrix}.$$

Ejemplo 3. Si $n \geq 3$, el grupo S_n no es abeliano. Por ejemplo, S_3 es un grupo de orden $3! = 6$ y sus elementos son:

$$\mathrm{id}_3 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \quad \sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \quad \sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix},$$

$$\sigma_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \quad \sigma_4 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \quad \sigma_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix},$$

y observe que

$$\sigma_4\sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = \sigma_5$$

y

$$\sigma_1\sigma_4 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \sigma_2$$

por lo que $\sigma_4\sigma_1 \neq \sigma_1\sigma_4$. Observe que este ejemplo sirve para cualquier $n \geq 3$. Explique (ejercicio).

Ejemplo 4. Los grupos S_1 y S_2 son sencillos:

$$\begin{aligned} S_1 &= \{e\} \\ S_2 &= \left\{e = \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}, \sigma = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}\right\}, \end{aligned}$$

es decir, S_1 es el grupo trivial, y observamos que el elemento $\sigma \in S_2$ satisface que

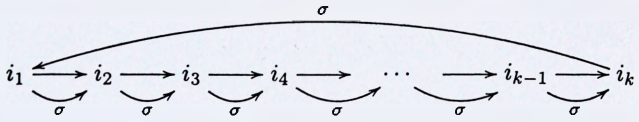
$$\sigma^2 = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix} = e,$$

i.e., $\sigma^2 = e$ por lo que σ es de orden 2. Se sigue que el subgrupo cíclico generado por σ es todo S_2, i.e., $\langle\sigma\rangle = S_2$ y por lo tanto S_2 es cíclico.

Ciclos y órbitas. Si $\sigma \in S_n$ es una permutación y $x \in \mathbb{I}_n$ es un elemento, diremos que σ *fija* a x si $\sigma(x) = x$. En caso contrario, diremos que σ *mueve* a x. Ahora, si $i_1, i_2, \ldots, i_k$ son enteros distintos de $\mathbb{I}_n$ y si $\sigma \in S_n$ es tal que

$$\sigma(i_1) = i_2, \sigma(i_2) = i_3, \ldots, \sigma(i_{k-1}) = i_k, \sigma(i_k) = i_1$$

y σ fija a los otros enteros de $\mathbb{I}_n$, si los hay, entonces, diremos que σ es un *ciclo de longitud k* ó un *k-ciclo*. La etimología circular proviene de observar que:



(donde las flechas curvas denotan la aplicación de σ al elemento i_j considerado) y como $\sigma(x) = x$, para toda $x \neq i_1, i_2, \ldots, i_k$, entonces en lugar de la notación usual para una permutación arbitraria:

$$\sigma = \begin{pmatrix} \cdots & i_1 & \cdots & i_2 & \cdots & x & \cdots \\ \cdots & i_2 & \cdots & i_3 & \cdots & x & \cdots \end{pmatrix}$$

usaremos la notación abreviada:

$$\sigma = (i_1, i_2, i_3, \ldots, i_{k-1}, i_k)$$

pensando a σ como una k-ada ordenada, donde se entiende que el ciclo σ manda el número de la izquierda al número de la derecha y al llegar al último, el número i_k va a dar al inicio del ciclo, i.e., a i_1. Se sobreentiende que los números $x \in \mathbb{I}_n$ que no están en la k-ada anterior, son fijados por σ. Una convención más, los 1-ciclos son de la forma $\sigma = (x)$, donde se entiende que la permutación σ fija a los enteros de $\mathbb{I}_n$ no listados en el ciclo $\sigma = (x)$, i.e., fija a todos excepto posiblemente a x y por lo tanto también fija a x. Es decir, $\sigma = \mathrm{id}_n$, por lo que todos los 1-ciclos son iguales a la permutación identidad, a la cual algunas veces denotamos por $\mathrm{id}_n = (1)$.

Ejemplo 5. En S_5 tenemos el ciclo $\sigma = (2, 4, 1)$ que como permutación es:

$$\sigma = (2,4,1) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 3 & 1 & 5 \end{pmatrix}$$

notando que σ fija a los enteros 3 y 5.

Sea $\sigma \in S_n$ una permutación. Para un elemento dado $x \in \mathbb{I}_n$, el conjunto

$$\mathcal{O}_\sigma(x) := \{\sigma^k(x) \ : \ k \in \mathbb{Z}\}$$

se llamará la *órbita de x bajo σ*.

Ejemplo 6. Si $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix} \in S_4$ y $x = 2 \in \mathbb{I}_4$, para obtener la órbita correspondiente, calculamos: $\sigma^0(2) = 2$, $\sigma(2) = 3$, $\sigma^2(2) = \sigma(3) = 1$, $\sigma^3(2) = \sigma(1) = 2$ y luego se repiten los valores (por eso es una *órbita*, i.e., se repiten los valores dando vueltas). Por lo tanto, la órbita es:

$$\mathcal{O}_\sigma(2) = \{2, 3, 1\}.$$

Con la misma permutación σ y ahora con el entero $x = 4$, para obtener la órbita correspondiente calculamos $\sigma^0(4) = 4$, $\sigma(4) = 4$ y se repiten los valores, por lo que:

$$\mathcal{O}_\sigma(4) = \{4\}.$$

Los ejemplos anteriores muestran cómo se calcula la órbita de un elemento x para una permutación σ dada: primero observamos que $x \in \mathcal{O}_\sigma(x)$ ya que $\sigma^0(x) = x$. Después, nos fijamos en el lugar en que está x en el renglón superior (el dominio) de σ y por lo tanto debajo de éste x se encuentra el valor $\sigma(x)$. Luego, localizamos el valor $\sigma(x)$ en el renglón superior de σ y por lo tanto debajo de él se encuentra el valor $\sigma(\sigma(x)) = \sigma^2(x)$. El proceso anterior se aplica hasta que aparezcan repeticiones.

Ejemplo 7. Si $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 1 & 4 & 6 & 5 \end{pmatrix} \in S_6$, entonces todas sus órbitas son:

$$\begin{aligned} \mathcal{O}_\sigma(1) &= \{1, 2, 3\} = \mathcal{O}_\sigma(2) = \mathcal{O}_\sigma(3) \\ \mathcal{O}_\sigma(4) &= \{4\} \\ \mathcal{O}_\sigma(5) &= \{5, 6\}. \end{aligned}$$

El ejemplo anterior ilustra las propiedades generales siguientes:

LEMA 4.2. *Sea $\sigma \in S_n$ una permutación. Entonces,*

(1) *Ninguna órbita es vacía, ya que $x \in \mathcal{O}_\sigma(x)$.*
(2) *Las órbitas de σ son disjuntas, i.e., si $\mathcal{O}_\sigma(x) \cap \mathcal{O}_\sigma(z) \neq \emptyset$, entonces $\mathcal{O}_\sigma(x) = \mathcal{O}_\sigma(z)$.*
(3) *La unión de todas las órbitas es $\mathbb{I}_n$.*

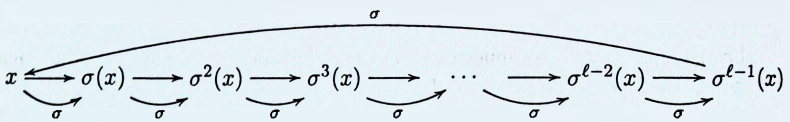
En otras palabras, si $\sigma \in S_n$, entonces el conjunto de órbitas $\mathcal{O}_\sigma(x)$, con x variando en $\mathbb{I}_n$, es una partición *de $\mathbb{I}_n$.*

Demostración. (1). Para cualquier $x \in \mathbb{I}_n$ se tiene que $x = \sigma^0(x) \in \mathcal{O}_\sigma(x)$.
(2). Si $w \in \mathcal{O}_\sigma(x) \cap \mathcal{O}_\sigma(z)$, entonces existen enteros $r, s \geq 0$ tales que $\sigma^r(x) = w = \sigma^s(z)$ y, sin perder generalidad, podemos asumir que $r \geq s$, por lo que $\sigma^{r-s}(x) = z$, i.e., $z \in \mathcal{O}_\sigma(x)$ y por lo tanto, para todo $k \in \mathbb{Z}$ se tiene que $\sigma^k(z) = \sigma^k(\sigma^{r-s}(x)) = \sigma^{k+r-s}(x) \in \mathcal{O}_\sigma(x)$, i.e, $\mathcal{O}_\sigma(z) \subseteq \mathcal{O}_\sigma(x)$. En forma similar se muestra que $\mathcal{O}_\sigma(x) \subseteq \mathcal{O}_\sigma(z)$. Las dos inclusiones anteriores dan la igualdad deseada.
(3). Como cada $\mathcal{O}_\sigma(z) \subseteq \mathbb{I}_n$, se tiene que $\bigcup \mathcal{O}_\sigma(z) \subseteq \mathbb{I}_n$. Recíprocamente, si $x \in \mathbb{I}_n$, entonces $x \in \mathcal{O}_\sigma(x) \subseteq \bigcup \mathcal{O}_\sigma(z)$ y por lo tanto $\mathbb{I}_n \subseteq \bigcup \mathcal{O}_\sigma(z)$. □

Observación. Dada $\sigma \in S_n$, como S_n es un grupo finito de orden $n!$, entonces σ es (un elemento) de orden finito también, i.e., existe un $1 \leq k \leq n!$ menor tal que $\sigma^k = e$, y por lo tanto $\sigma^k(x) = x$ para todo $x \in \mathbb{I}_n$. Así, dado el elemento $x \in \mathbb{I}_n$, existe un entero positivo menor ℓ con $1 \leq \ell \leq k \leq n!$ tal que $\sigma^\ell(x) = x$, y por lo tanto la órbita $\mathcal{O}_\sigma(x)$ de x está dada por:

$$x, \sigma(x), \sigma^2(x), \ldots, \sigma^{\ell-1}(x), \quad \text{(ya que } \sigma^\ell(x) = x\text{)}.$$

Note lo circular del conjunto anterior, o mejor, gráficamente:



donde notamos la fuerte similaridad con lo que sucede con los ciclos de longitud ℓ que estudiamos previamente. Es decir, a la órbita $\mathcal{O}_\sigma(x)$ le corresponde el ℓ-ciclo

$$(x, \sigma(x), \sigma^2(x), \ldots, \sigma^{\ell-1}(x)).$$

Hemos así probado:

PROPOSICIÓN 4.3. *Si $\sigma \in S_n$ y $x \in \mathbb{I}_n$, entonces la restricción $\sigma|_{\mathcal{O}_\sigma(x)}$ es un ciclo de longitud la cardinalidad de la órbita $\mathcal{O}_\sigma(x)$.*

□

La órbita correspondiente a un ciclo $\sigma = (i_1, i_2, \ldots, i_k)$ es el conjunto

$$\{i_1, i_2, \ldots, i_k\} = \mathcal{O}_\sigma(i_t), \quad \text{para } 1 \leq t \leq k.$$

Observemos que, un ciclo es un k-ciclo si la órbita correspondiente tiene cardinalidad k. Nótese también que el ciclo correspondiente a una órbita de cardinal uno $\{x\}$ es la identidad. También notamos que cuando decimos que un elemento $x \in \mathbb{I}_n$ está fijo bajo σ, lo que queremos decir es que su órbita es $\mathcal{O}_\sigma(x) = \{x\}$.

Dos permutaciones $\sigma, \tau \in S_n$ se dice que son *disjuntas* si para toda $x \in \mathbb{I}_n$, siempre que σ mueve a x, τ lo fija y viceversa. Es decir, si $\sigma(x) \neq x$, entonces $\tau(x) = x$ y si $\tau(z) \neq z$, entonces $\sigma(z) = z$. Dicho en otras palabras, dos permutaciones $\sigma, \tau \in S_n$ son disjuntas si y sólo si para toda $x \in \mathbb{I}_n$, las órbitas $\mathcal{O}_\sigma(x)$ y $\mathcal{O}_\tau(x)$ son disjuntas.

PROPOSICIÓN 4.4. *Si $\sigma, \tau \in S_n$ son dos permutaciones disjuntas, entonces $\sigma\tau = \tau\sigma$.*

Demostración. Sea $x \in \mathbb{I}_n$. Mostraremos que $\sigma\tau(x) = \tau\sigma(x)$. En efecto, si $\tau(x) \neq x$, entonces $\sigma(x) = x$ y así

$$\tau\sigma(x) = \tau(x). \tag{1}$$

Ahora, como $\mathcal{O}_\tau(\tau(x)) = \mathcal{O}_\tau(x)$, entonces τ mueve a $\tau(x)$ por lo que σ lo fija, i.e., $\sigma(\tau(x)) = \tau(x)$. Se sigue que

$$\sigma\tau(x) = \tau(x). \tag{2}$$

Las igualdades (1) y (2) implican que $\sigma\tau(x) = \tau\sigma(x)$, en el caso cuando τ mueve a x. Si σ mueve a x el argumento es similar. Finalmente, si σ y τ fijan a x el resultado es trivial. Se sigue que $\sigma\tau = \tau\sigma$. □

Ejemplo 8. Observe que la condición de que las permutaciones sean disjuntas es indispensable ya que las permutaciones $\sigma = (1,3)$ y $\tau = (1,2)$ (de S_3) no son disjuntas y

$$\sigma\tau = (1,3)(1,2) = (1,2,3) \neq (1,3,2) = (1,2)(1,3) = \tau\sigma.$$

Nuestro objetivo ahora será mostrar que los ciclos son los ladrillos a partir de los cuales se construyen todas las permutaciones. Lo que queremos decir con ésto es que cualquier permutación $\sigma \in S_n$ que no sea la identidad, es producto de ciclos disjuntos en forma esencialmente única:

TEOREMA 4.5. *Toda permutación $\sigma \neq \mathrm{id}_n$ en S_n es el producto de ciclos disjuntos de longitud ≥ 2. Esta factorización es única salvo por el orden en el aparecen los ciclos correspondientes.*

Demostración. Mostraremos primero la *existencia* de la factorización de σ. Para esto, sean $\mathcal{O}_1, \mathcal{O}_2, \ldots, \mathcal{O}_k$ las órbitas de σ. Por la proposición 4.3 anterior las restricciones $\sigma|_{\mathcal{O}_j}$ son ciclos de longitud $\ell_j = |\mathcal{O}_j|$. Definamos la permutación $\kappa_j \in S_n$ mediante la función que fija a los elementos fuera de la órbita $\mathcal{O}_j$ y que es igual a $\sigma|_{\mathcal{O}_j}$ en $\mathcal{O}_j$. Entonces, κ_j es un ciclo de S_n, para cada $j = 1, \ldots, k$. Más aún, como las órbitas $\mathcal{O}_j$ son disjuntas, los ciclos κ_j son disjuntos por pares. Finalmente, como los ciclos κ_j son disjuntos al evaluar el producto $\kappa_1\kappa_2\cdots\kappa_k$ en cualquier $x \in \mathbb{I}_n$ sólo importa el ciclo κ_j cuya órbita $\mathcal{O}_j$ contiene al elemento x ya que los otros κ_i, $i \neq j$, lo fijan. Ahora, $\kappa_j(x) = \sigma|_{\mathcal{O}_j}(x)$ y por lo tanto

$$\sigma = \kappa_1\kappa_2\cdots\kappa_k,$$

es la factorización deseada, si previamente se eliminaron los factores κ_t iguales a la identidad.

Para probar la *unicidad* de la factorización anterior, supongamos que

$$\sigma = \kappa_1\kappa_2\cdots\kappa_k = \gamma_1\gamma_2\cdots\gamma_m, \tag{*}$$

donde las κ_j y las γ_i son ciclos disjuntos de longitud ≥ 2.

Supongamos ahora que σ mueve al elemento $x \in \mathbb{I}_n$. Entonces exactamente uno de los κ_i mueve a x y exactamente uno de los γ_j mueve a x. Como los ciclos son disjuntos, conmutan por la proposición 4.4, y así, sin perder generalidad, podemos

asumir que los ciclos que mueven a x son κ_1 y γ_1, respectivamente. Ahora, como $\kappa_1(x) = \sigma(x) = \gamma_1(x)$, entonces para cualquier entero t se tiene que

$$\kappa_1^t(x) = \sigma^t(x) = \gamma_1^t(x)$$

y como los ciclos están determinados por sus potencias evaluadas en cualquier elemento que mueven, entonces la igualdad anterior implica que $\kappa_1 = \gamma_1$. Podemos entonces cancelar los primeros factores en $(*)$. La demostración se concluye por inducción. □

Ejemplo 9. Para la permutación $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 6 & 4 & 7 & 2 & 5 & 1 & 8 & 9 & 3 \end{pmatrix}$, sus órbitas son:

$$\mathcal{O}_1 = \{1,6\}, \mathcal{O}_2 = \{2,4\}, \mathcal{O}_3 = \{3,7,8,9\}, \mathcal{O}_4 = \{5\}$$

por lo que la factorización de σ en ciclos disjuntos es:

$$\sigma = (1,6)(2,4)(3,7,8,9).$$

Ejemplo 10. No está por demás recordar que para multiplicar ciclos de S_n lo hacemos de derecha a izquierda, tomando un elemento (de $\mathbb{I}_n$) del ciclo más a la derecha que lo contenga y viendo cómo se transforma siguiendo el orden de las permutaciones hacia la izquierda. Por ejemplo, para calcular el producto de ciclos de S_5:

$$(1,2)(2,4,5)(1,3)(1,2,5)$$

calculamos de derecha a izquierda:

$$\begin{array}{lll} 1 \mapsto 2 \mapsto 2 \mapsto 4 \mapsto 4 & \text{por lo que} & 1 \mapsto 4 \\ 2 \mapsto 5 \mapsto 5 \mapsto 2 \mapsto 1 & \text{por lo que} & 2 \mapsto 1 \\ 3 \mapsto 3 \mapsto 1 \mapsto 1 \mapsto 2 & \text{por lo que} & 3 \mapsto 2 \\ 4 \mapsto 4 \mapsto 4 \mapsto 5 \mapsto 5 & \text{por lo que} & 4 \mapsto 5 \\ 5 \mapsto 1 \mapsto 3 \mapsto 3 \mapsto 3 & \text{por lo que} & 5 \mapsto 3 \end{array}$$

y así

$$(1,2)(2,4,5)(1,3)(1,2,5) = (1,4,5,3,2).$$

(Aunque aquí el producto de ciclos resultó un ciclo, en general esto no tiene por qué suceder).

Permutaciones pares e impares. Un 2-ciclo de S_n se llama una *transposición*. Note la simplicidad de las transposiciones, ya que sólo mueven dos elementos de $\mathbb{I}_n$. Si $\tau = (a,b)$ es una transposición de S_n, entonces su inversa, como permutación, es ella misma ya que

$$\tau\tau(a) = \tau(b) = a \quad \text{y} \quad \tau\tau(b) = \tau(a) = b,$$

y los otros elementos $z \in \mathbb{I}_n$ están fijos bajo τ y consecuentemente bajo τ^2 también. Hemos así mostrado que τ^2 fija a *todos* los elementos de $\mathbb{I}_n$ y por lo tanto $\tau^2 = \mathrm{id}_n$, i.e., $\tau^{-1} = \tau$.

Observemos ahora que todo ciclo no trivial $(a_1, a_2, \ldots, a_k) \in S_n$ se puede escribir como producto de transposiciones de la forma:

$$(a_1, a_2, \ldots, a_k) = (a_1, a_k)(a_1, a_{k-1}) \cdots (a_1, a_3)(a_1, a_2),$$

tan sólo notando que la composición se hace de derecha a izquierda. Aplicando ésto al teorema 4.5, hemos así probado:

TEOREMA 4.6. *Toda permutación σ en S_n es producto de transposiciones.*

□

Note sin embargo que la factorización anterior no es tan buena como la del teorema 4.5 en ciclos disjuntos ya que, en primer lugar, las transposiciones involucradas no necesariamente conmutan. Por ejemplo,

$$(1,3)(1,2) = (1,2,3) \neq (1,3,2) = (1,2)(1,3).$$

En segundo lugar, los factores no están unívocamente determinados, por ejemplo,

$$\begin{aligned}(1,2,3) &= (1,3)(1,2) = (2,3)(1,3) = (1,3)(4,2)(1,2)(1,4)\\ &= (1,3)(4,2)(1,2)(1,4)(2,3)(2,3).\end{aligned}$$

¿Qué es lo que no cambia en estas factorizaciones? Probaremos a continuación que lo que no cambia es la *paridad* del número de transposiciones involucradas, es decir, que dada σ al factorizarla en transposiciones siempre se tiene un número par de ellas o siempre un número impar (en el ejemplo anterior el número de transposiciones es *par*).

Para comenzar a probar ésto, dada una permutación $\sigma \in S_n$, denotemos con $|\sigma|$ al *número de órbitas* de σ y observemos que si $\tau = (a, b) \in S_n$ es cualquier transposición, entonces

$$|\tau\sigma| = |\sigma| \pm 1,$$

y para probar ésto notamos primero que las órbitas de σ que no contienen ni a a ni a b, no son afectadas al multiplicar τ por σ, i.e., también son órbitas de $\tau\sigma$. Basta entonces considerar las órbitas de σ que contienen a a ó b, y tenemos dos casos:

CASO 1. Supongamos que a y b pertenecen a una misma órbita de σ por lo que el ciclo correspondiente tiene la forma $(a, c_1, \ldots, c_j, b, d_1, \ldots, d_k)$ (note que siempre podemos asumir que el ciclo comienza en a porque para cualquier ciclo se tiene la igualdad: $(i_1, i_2, \ldots, i_{k-1}, i_k) = (i_k, i_1, i_2, \ldots, i_{k-1})$). Multiplicando el ciclo anterior por la transposición $\tau = (a, b)$ a la izquierda, queda

$$(1) \qquad (a,b)(a, c_1, \ldots, c_j, b, d_1, \ldots, d_k) = (a, c_1, \ldots, c_j)(b, d_1, \ldots, d_k)$$

ya que el lado izquierdo de (1) manda:

$$a \mapsto c_1 \mapsto c_1; \quad c_i \mapsto c_{i+1} \mapsto c_{i+1} \quad \text{para } i < j; \quad c_j \mapsto b \mapsto a$$

y

$$b \mapsto d_1 \mapsto d_1; \quad d_i \mapsto d_{i+1} \mapsto d_{i+1} \quad \text{para } i < k; \quad d_k \mapsto a \mapsto b$$

que es igual a lo que hace el lado derecho de (1). Hemos así mostrado que al multiplicar el ciclo que contiene a a y a b por (a, b) se rompe el ciclo dado en dos ciclos disjuntos de $\tau\sigma$ y por lo tanto $|\tau\sigma| = |\sigma| + 1$.

CASO 2. Supongamos ahora que a, b pertenecen a dos ciclos disjuntos de σ, digamos $(a, c_1, \ldots, c_j)$ y $(b, d_1, \ldots, d_k)$. Queremos ver cómo es el producto

$$(a, b)(a, c_1, \ldots, c_j)(b, d_1, \ldots, d_k)$$

y para ésto multipliquemos los dos lados de (1) por $\tau = (a, b)$ a la izquierda, recordando que $\tau^2 = \mathrm{id}$:

$$\begin{aligned}(a, c_1, \ldots, c_j, b, d_1, \ldots, d_k) &= (a, b)(a, b)(a, c_1, \ldots, c_j, b, d_1, \ldots, d_k) \\ &= (a, b)(a, c_1, \ldots, c_j)(b, d_1, \ldots, d_k)\end{aligned}$$

notando que se obtiene un sólo ciclo (el de la izquierda) y por lo tanto los dos ciclos se fusionaron y así $|\tau\sigma| = |\sigma| - 1$.

Una consecuencia inmediata de la igualdad $|\tau\sigma| = |\sigma| \pm 1$ que acabamos de probar es que si definimos la función *signo* $\operatorname{sgn} : S_n \to \{\pm 1\}$ mediante

$$\operatorname{sgn}(\sigma) := (-1)^{n-|\sigma|},$$

entonces para cualquier transposición $\tau \in S_n$ se tiene que

$$(*) \qquad \operatorname{sgn}(\tau\sigma) = -\operatorname{sgn}(\sigma).$$

Observe ahora que para la permutación $\mathrm{id} \in S_n$, sus órbitas son de la forma $\{i\}$ para $i \in \mathbb{I}_n$ por lo que $|\,\mathrm{id}\,| = n$ y así $\operatorname{sgn}(\mathrm{id}) = (-1)^{n-n} = 1$. Poniendo $\sigma = \mathrm{id}$ en $(*)$ se sigue que si $\tau \in S_n$ es cualquier transposición, entonces $\operatorname{sgn}(\tau) = -1$, y en general, si $\tau_1, \ldots, \tau_k \in S_n$ son transposiciones, inducción sobre k usando $(*)$ implica que

$$\operatorname{sgn}(\tau_1 \cdots \tau_k) = (-1)^k,$$

y por lo tanto, para cualquier permutación $\sigma \in S_n$, si la factorizamos, usando 4.6, como producto de transposiciones $\sigma = \tau_1 \cdots \tau_k$, se tiene que

$$\operatorname{sgn}(\sigma) = (-1)^k$$

y como el valor de la parte izquierda sólo depende de σ, entonces el número k de transposiciones en cualquier factorización 4.6 de σ mantiene su paridad. Hemos así probado:

TEOREMA 4.7. *Si $\sigma \in S_n$, el número de transposiciones que aparecen en cualquier factorización* (del teorema 4.6) *de σ, siempre es par o siempre es impar.* □

Una permutación σ se dice que es *par* si en cualquier factorización, como producto de transposiciones, el número de éstas es par. En caso contrario se dirá que σ es *impar*.

COROLARIO 4.8. (1) *Si* $\sigma, \vartheta \in S_n$, *entonces* $\operatorname{sgn}(\sigma\vartheta) = \operatorname{sgn}(\sigma)\operatorname{sgn}(\vartheta)$.

(2) *Si* $\sigma \in S_n$, *entonces* $\operatorname{sgn}(\sigma^{-1}) = \operatorname{sgn}(\sigma)$.

□

El grupo alternante. Denotemos con A_n al conjunto de todas las permutaciones pares de S_n. Como la identidad id_n es una permutación par, entonces $\mathrm{id}_n \in A_n$. También, como por 4.8 el producto de dos permutaciones pares es par, A_n es cerrado bajo el producto de S_n. Finalmente, la inversa de una permutación par, también es par por el corolario 4.8 y así $A_n \subseteq S_n$ es un subgrupo, al que se conoce como el *grupo alternante* de grado n.

PROPOSICIÓN 4.9. *Hay tantas permutaciones pares como impares. Por lo tanto el orden del grupo alternante* A_n *es* $n!/2$.

Demostración. Sea $n \geq 2$ (para que hayan transposiciones). Fijemos la transposición $\tau = (1,2) \in S_n$ y sea B_n el conjunto de permutaciones impares. Definamos la función

$$\widehat{\tau} : A_n \to B_n$$

mediante $\widehat{\tau}(\sigma) := \sigma\tau$. Observamos que como σ es par y τ es impar, entonces $\sigma\tau$ es impar, i.e., $\sigma\tau \in B_n$ por lo que $\widehat{\tau}$ está bien definida. Mostraremos que $\widehat{\tau}$ es biyectiva. Para comenzar, es inyectiva ya que si $\widehat{\tau}(\sigma) = \widehat{\tau}(\alpha)$, entonces $\sigma\tau = \alpha\tau$ y cancelando la τ a la derecha queda $\sigma = \alpha$. Es suprayectiva, ya que si $\beta \in B_n$ es una permutación impar, entonces $\beta\tau$ es una permutación par, i.e., $\beta\tau \in A_n$ y satisface que $\widehat{\tau}(\beta\tau) = \beta\tau\tau = \beta$. □

Ejemplo 11. El grupo alternante A_3 de S_3 está dado por las permutaciones

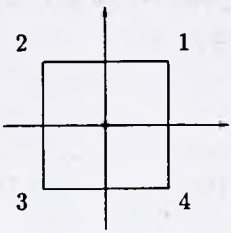
$$A_3 = \left\{ \mathrm{id}_3 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \quad \sigma_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \quad \sigma_4 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \right\},$$

ya que

$$\sigma_3 = (1,2,3) = (1,3)(1,2) \quad \text{y} \quad \sigma_4 = (1,3,2) = (1,2)(1,3)$$

son permutaciones pares.

El grupo diédrico. Si denotamos con D_8 al grupo de simetrías del cuadrado, los elementos de D_8 son las cuatro *rotaciones* r^k, $0 \leq k < 4$ (por ángulos de 0, 90, 180, y 270 grados) y las cuatro *reflexiones*, ρ_i, $1 \leq i \leq 4$ (dos respecto a los ejes coordenados y dos con respecto a las diagonales del cuadrado). Así, los elementos del grupo D_8 mueven los cuatro vértices del cuadrado colocándolos encima de ellos, de tal forma que si etiquetamos los vértices con los números 1, 2, 3, 4:



los elementos de D_8 se pueden pensar como algunas de las permutaciones del conjunto $\mathbb{I}_4$, i.e., D_8 es un *subgrupo* de S_4. De hecho, podemos identificar las 8 permutaciones de S_4 que pertenecen a D_8. Éstas son:

$$e = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}$$ la identidad

$$r = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$$ la rotación $r_{\pi/2}$

$$r^2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$$ la rotación $r_\pi = r^2_{\pi/2}$

$$r^3 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}$$ la rotación $r_{3\pi/2} = r^3_{\pi/2}$

$$\rho_Y = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$$ la reflexión ρ alrededor del eje Y

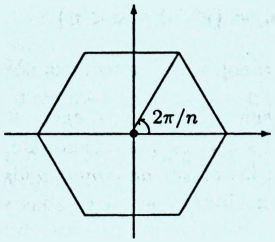
$$\rho_X = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}$$ la reflexión alrededor del eje X

$$\rho_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix}$$ la reflexión a 45 grados

$$\rho_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}$$ la reflexión a 135 grados.

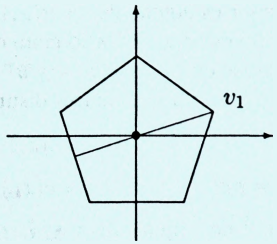
En general, si se tiene un *polígono regular de n lados* centrado en el origen de $\mathbb{R}^2$, digamos con uno de sus lados paralelo al eje X, y si consideramos sus simetrías, es decir, etiquetando sus vértices con los enteros del 1 al n, consecutivamente en sentido contrario al de las manecillas de un reloj, las simetrías serán los movimientos del polígono que llevan sus n vértices en los n vértices del mismo y por lo tanto las podemos considerar como (algunas) de las permutaciones de $\mathbb{I}_n$, i.e., como elementos de S_n. Dicho en otras palabras, el *grupo de simetrías* D_{2n} de un polígono regular de n lados es un subgrupo del grupo simétrico S_n.

Observemos ahora que las simetrías del polígono incluyen las n rotaciones r^k, donde $r = r_{2\pi/n}$ es la rotación por el ángulo $2\pi/n$ y $0 \leq k < n$:

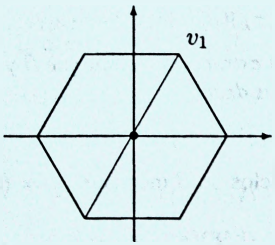


Además de las rotaciones también se tienen las simetrías dadas por las *reflexiones*:

• Si n es *impar*, el grupo D_{2n} contiene las n *reflexiones* con respecto a las bisectrices de los ángulos internos del polígono:



• Si n es *par*, el grupo D_{2n} contiene las $n/2$ reflexiones con respecto a las bisectrices de sus ángulos internos (note que sólo hay $n/2$ de éstas) y las $n/2$ reflexiones con respecto a las rectas que bisectan los lados del polígono (note también que hay $n/2$ de éstas):



El argumento geométrico anterior sugiere que D_{2n} es el subgrupo de S_n dado por:

$$D_{2n} = \{r^k,\ 0 \leq k < n,\ \rho_1, \rho_2, \ldots, \rho_n\},$$

por lo que su orden es $2n$. El grupo D_{2n} se llama el *grupo diédrico* de orden $2n$. Observe que D_{2n} contiene al subgrupo $R_n \subseteq D_{2n}$ formado por las rotaciones

$$R_n = \{r^k,\ 0 \leq k < n\}$$

y el orden de R_n es n.

Clases de conjugación en S_n. Dados $\sigma, \tau \in S_n$, si existe $\theta \in S_n$ tal que $\sigma = \theta\tau\theta^{-1}$, se dice que σ es *conjugada* de τ y ésta es una relación de equivalencia en S_n cuyas clases de equivalencia se llaman las *clases de conjugación* de S_n. Nuestro objetivo es determinar cuándo dos permutaciones son conjugadas y éste es el contenido del teorema 4.12:

LEMA 4.10. *Sea $c = (x_1, x_2, \ldots, x_k) \in S_n$ un k-ciclo. Entonces, para toda $\sigma \in S_n$ el elemento $\sigma c \sigma^{-1}$ también es un k-ciclo y se tiene que*

$$\sigma c \sigma^{-1} = (\sigma(x_1), \sigma(x_2), \ldots, \sigma(x_k)).$$

Demostración. Si $x \in \mathbb{I}_n$, entonces x es alguno de los $\sigma(x_i)$ o no lo es. Si x no es de la forma $\sigma(x_i)$, entonces $\sigma^{-1}(x)$ no es un x_i y por lo tanto el ciclo c lo deja fijo, i.e., $c\sigma^{-1}(x) = \sigma^{-1}(x)$, de donde se sigue que $\sigma c \sigma^{-1}(x) = \sigma\sigma^{-1}(x) = x$.

Por otra parte, si x es alguno de los $\sigma(x_i)$, entonces distinguimos dos casos:

(1) Si $i < k$, entonces $\sigma c \sigma^{-1}(x) = \sigma c \sigma^{-1}(\sigma(x_i)) = \sigma c(x_i) = \sigma(x_{i+1})$.

(2) Si $i = k$, entonces $\sigma c \sigma^{-1}(x) = \sigma c \sigma^{-1}(\sigma(x_k)) = \sigma c(x_k) = \sigma(x_1)$.

Hemos así mostrado que $\sigma c \sigma^{-1}$ deja fijos a los $x \in \mathbb{I}_n$ que no son de los $\sigma(x_i)$ y actúa en las x que sí son de los $\sigma(x_i)$ como el ciclo $(\sigma(x_1), \ldots, \sigma(x_n))$. Se sigue que $\sigma c \sigma^{-1}$ debe ser este ciclo. □

PROPOSICIÓN 4.11. *Sean $\alpha, \beta \in S_n$ y supongamos que β tiene la descomposición en ciclos disjuntos*

$$\beta = (x_1, \ldots, x_k)(y_1, \ldots, y_\ell) \cdots (z_1, \ldots, z_m).$$

Entonces, $\alpha\beta\alpha^{-1}$ tiene la misma estructura cíclica que β y se obtiene aplicando α a los símbolos en cada ciclo de β, es decir,

$$\alpha\beta\alpha^{-1} = (\alpha(x_1), \ldots, \alpha(x_k))(\alpha(y_1), \ldots, \alpha(y_\ell)) \cdots (\alpha(z_1), \ldots, \alpha(z_m)).$$

Demostración. Denotemos los ciclos de β mediante $c_j = (x_1, \ldots, x_k)$, de tal forma que $\beta = c_1 c_2 \cdots c_t$. Entonces,

$$\alpha\beta\alpha^{-1} = \alpha(c_1 c_2 \cdots c_t)\alpha^{-1} = (\alpha c_1 \alpha^{-1})(\alpha c_2 \alpha^{-1}) \cdots (\alpha c_t \alpha^{-1})$$

y por el lema anterior cada uno de los factores $(\alpha c_j \alpha^{-1})$ es un ciclo que se obtiene aplicando α a los elementos del ciclo c_j. El resultado se sigue. □

Ejemplo 12. Si $\alpha = (13)(246)$ y si $\beta = (16)(24)(357)$, entonces

$$\alpha\beta\alpha^{-1} = (\alpha(1)\alpha(6))(\alpha(2)\alpha(4))(\alpha(3)\alpha(5)\alpha(7)) = (32)(46)(157).$$

Cuando en la proposición anterior decimos que permutaciones conjugadas tienen la misma estructura cíclica, queremos decir que en su descomposición como productos de ciclos disjuntos, del teorema 4.5, aparece el mismo número de ciclos en cada permutación y éstos son del mismo tamaño en ambas permutationes. La recíproca de la proposición anterior también es válida:

TEOREMA 4.12. *Dos permutaciones $\alpha, \beta \in S_n$ tienen la misma estructura cíclica si y sólo si son conjugadas.*

Demostración. Sólo falta probar que si α y β tienen la misma estructura cíclica, entonces son conjugadas. Para ésto, supongamos que

$$\alpha = (x_1, \ldots, x_k)(y_1, \ldots, y_\ell)\cdots(z_1, \ldots, z_m),$$
$$\beta = (x'_1, \ldots, x'_k)(y'_1, \ldots, y'_\ell)\cdots(z'_1, \ldots, z'_m).$$

Queremos encontrar un $\theta \in S_n$ tal que $\theta\alpha\theta^{-1} = \beta$ y como por el lema previo

$$\theta\alpha\theta^{-1} = (\theta x_1, \ldots, \theta x_k)(\theta y_1, \ldots, \theta y_\ell)\cdots(\theta z_1, \ldots, \theta z_m),$$

entonces queremos un θ tal que

$$(\theta x_1 \ldots \theta x_k)(\theta y_1 \ldots \theta y_\ell)\cdots(\theta z_1 \ldots \theta z_m) = (x'_1 \ldots x'_k)(y'_1 \ldots y'_\ell)\cdots(z'_1 \ldots z'_m)$$

y así basta probar que existe un $\theta \in S_n$ tal que

$$(*) \qquad \theta x_i = x'_i; \quad \theta y_i = y'_i; \quad \theta z_i = z'_i$$

lo cual es obvio si se observa que los ciclos de α son disjuntos y los mismo pasa para β, por lo que el número de elementos que α deja fijos es igual al número de elementos que β deja fijos, se sigue que podemos definir $\theta : \mathbb{I}_n \to \mathbb{I}_n$ mediante $(*)$ para los elementos de $\mathbb{I}_n$ que aparecen en algún ciclo de α y como $\theta(x) = x'$ si x no aparece en α y donde x' es cualquier elemento de $\mathbb{I}_n$ que no aparece en β. □

Ejemplo 13. Las permutaciones $\alpha = (26)(13)(457)$ y $\beta = (16)(24)(358)$ de S_8 tienen la misma estructura cíclica y poniéndolas una encima de la otra para definir $\theta \in S_8$ como en el teorema anterior:

$$\alpha = (26)(13)(457)$$
$$\beta = (16)(24)(358)$$

obtenemos

$$\theta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 1 & 4 & 3 & 5 & 6 & 8 & 7 \end{pmatrix}$$

donde observamos que el 8 no aparece en α y el 7 no aparece en β por lo que $\theta 8 = 7$. Comprobamos inmediatamente que

$$\theta\alpha\theta^{-1} = (\theta 2\ \theta 6)(\theta 1\ \theta 3)(\theta 4\ \theta 5\ \theta 7) = (16)(24)(358) = \beta.$$

El número de k-ciclos en S_n. Un k-ciclo en S_n es una ordenación (sin repetición) de k elementos de $\mathbb{I}_n$:

$$c = (x_1, x_2, \ldots, x_k)$$

y hay $n!/(n-k)!$ de estas ordenaciones. Sin embargo, recordemos que cada k-ciclo se puede escribir de k maneras distintas

$$(x_1, x_2, \ldots, x_k) = (x_k, x_1, x_2, \ldots, x_{k-1}) = \cdots = (x_2, x_3, \ldots, x_{k-1}, x_k, x_1)$$

y así, para contar los k-ciclos de S_n hay que dividir entre k el número de ordenaciones $n!/(n-k)!$, por lo que el número de k-ciclos en S_n es:

$$\frac{1}{k}\left(\frac{n!}{(n-k)!}\right) = \frac{1}{k}(n(n-1)\cdots(n-k+1)).$$

El número de estructuras cíclicas en S_n. Sean $c_i \geq 0$ enteros ($1 \leq i \leq k \leq n$). Una permutación $\sigma \in S_n$ se dice que es del *tipo* $(c_1, \ldots, c_k)$ si en la factorización de σ en ciclos disjuntos de S_n se tienen c_1 ciclos de longitud 1, c_2 ciclos de longitud 2, ..., c_k ciclos de longitud k, i.e.,

$$\sigma = \overbrace{(\bullet)\cdots(\bullet)}^{c_1}\overbrace{(\bullet\ \bullet)\cdots(\bullet\ \bullet)}^{c_2}\cdots\overbrace{(\underbrace{\bullet\ \bullet\ \bullet\ \bullet\ \bullet}_{k})\cdots(\underbrace{\bullet\ \bullet\ \bullet\ \bullet\ \bullet}_{k})}^{c_k}$$

donde $(\underbrace{\bullet\ \bullet\ \bullet\ \bullet\ \bullet}_{t})$ denota un t-ciclo. Note que por cada elemento de $\mathbb{I}_n$ que está fijo bajo σ se está contando el 1-ciclo correspondiente. Es claro entonces que

$$1 \cdot c_1 + 2 \cdot c_2 + \cdots + k \cdot c_k = n \tag{1}$$

y por convención escribimos los ciclos de σ del menor al mayor y también ponemos $c_j = 0$ si no hay j-ciclos en σ por lo que la ecuación anterior la podemos escribir como

$$1 \cdot c_1 + 2 \cdot c_2 + \cdots + n \cdot c_n = n. \tag{2}$$

Ahora, si ponemos

$$\mu_i := c_i + c_{i+1} + \cdots + c_n \tag{3}$$

entonces $\mu_1 \geq \mu_2 \geq \cdots \geq \mu_n \geq 0$ y de (1) se sigue que

$$\mu_1 + \mu_2 + \cdots + \mu_n = n, \tag{4}$$

es decir, los enteros $\mu_i \geq 0$ forman una *partición* del entero n (más precisamente, consideramos sólo los enteros positivos μ_i que sumados dan n). Recíprocamente, dada

una partición $(\mu_1, \ldots, \mu_k)$ de n con $\mu_1 \geq \mu_2 \geq \cdots \geq \mu_k \geq 0$ y $\sum_{i=1}^{k} \mu_i = n$, entonces poniendo

$$c_i := \mu_i - \mu_{i+1} \tag{5}$$

se tiene que los $c_i \geq 0$ y además $\sum_{i=1}^{n} i \cdot c_i = n$. Hemos así probado:

PROPOSICIÓN 4.13. *El número de tipos distintos de permutaciones en S_n es igual al número de particiones del entero n. Por el* teorema 4.12 *este número es igual al número de clases de conjugación en S_n.*

□

Ejemplo 14. Para S_4, las particiones de $n = 4$ son:

$$(1,1,1,1); \quad (1,1,2); \quad (1,3); \quad (2,2); \quad (4)$$

y por lo tanto S_4 tiene 5 clases de conjugación o, equivalentemente, 5 tipos de estructuras cíclicas. Es fácil listar las 5 estructuras cíclicas de S_4:

$(\bullet)$	1-ciclos	asociados a la partición $(1,1,1,1)$
$(\bullet\ \bullet)$	2-ciclos	asociados a la partición $(1,1,2)$
$(\bullet\ \bullet\ \bullet)$	3-ciclos	asociados a la partición $(1,3)$
$(\bullet\ \bullet\ \bullet\ \bullet)$	4-ciclos	asociados a la partición (4)
$(\bullet\ \bullet)(\bullet\ \bullet)$	productos de dos 2-ciclos	asociados a la partición $(2,2)$.

El número de permutaciones de un tipo dado. Nuestro objetivo ahora es contar cuántas permutaciones en S_n tienen un mismo tipo $(c_1, c_2, \ldots, c_n)$, donde ponemos $c_j = 0$ si no hay j-ciclos, es decir, queremos contar cuántos elementos tiene cada clase de conjugación de S_n. Ahora, estas permutaciones tienen la estructura cíclica

$$(*) \qquad \overbrace{(\bullet)\cdots(\bullet)}^{c_1}\ \overbrace{(\bullet\ \bullet)\cdots(\bullet\ \bullet)}^{c_2}\cdots\ \overbrace{(\underbrace{\bullet\ \bullet\ \bullet\ \bullet\ \bullet}_{n})\cdots(\underbrace{\bullet\ \bullet\ \bullet\ \bullet\ \bullet}_{n})}^{c_n}$$

donde $1 \cdot c_1 + 2 \cdot c_2 + \cdots + n \cdot c_n = n$ y como los ciclos son disjuntos, entonces los n elementos de $\mathbb{I}_n$ se tienen que repartir en las n casillas de $(*)$ por lo que hay $n!$ posibilidades para ubicar a estos elementos de $\mathbb{I}_n$ en el tipo $(*)$. Sin embargo, no todas estas distribuciones nos dan permutaciones distintas ya que:

(1) Como los ciclos de $(*)$ son disjuntos, los podemos permutar entre ellos y nos dan la misma permutación de S_n. Por ejemplo, para los 2-ciclos disjuntos $(a,b)(c,d) = (c,d)(a,b)$ por lo que los 2-ciclos se pueden permutar de $c_2!$ maneras y dan la misma partición de S_n. Similarmente para los otros k-ciclos y por lo tanto la misma partición se obtiene de

$$c_1! c_2! \cdots c_n!$$

formas distintas.

(2) Además, cada k-ciclo se puede escribir de k formas distintas:

$$(x_1, \ldots, x_k) = (x_k, x_1, \ldots, x_{k-1}) = \cdots = (x_2, \ldots, x_k, x_1),$$

por lo que los c_k ciclos de longitud k en el tipo $(*)$ están contados k^{c_k} veces y por lo tanto cada permutación del tipo $(*)$ está siendo contada

$$1^{c_1} \cdot 2^{c_2} \cdots n^{c_n}$$

veces.

Hemos así probado:

TEOREMA 4.14 (Fórmula de Cauchy). *El número de permutaciones distintas del tipo* $(*)$ *es:*

$$\frac{n!}{1^{c_1}c_1! \cdot 2^{c_2}c_2! \cdots n^{c_n}c_n!}.$$

□

Ejemplo 15. En S_4 consideremos el tipo correspondiente a la partición $(2,2)$ de $n = 4$, es decir, al tipo $(\bullet\ \bullet)(\bullet\ \bullet)$. Se tiene entonces que $c_1 = 0$, $c_2 = 2$, $c_3 = 0$, $c_4 = 0$, y la fórmula de Cauchy nos dice que hay

$$\frac{4!}{1^0 0! 2^2 2! 3^0 0! 4^0 0!} = \frac{4!}{4 \cdot 2!} = 3$$

permutaciones en S_4 del tipo $(\bullet\ \bullet)(\bullet\ \bullet)$, y éstas son:

$$(1,2)(3,4); \quad (1,3)(2,4); \quad (1,4)(2,3).$$

Ejemplo 16. En S_4 consideremos el tipo correspondiente a la partición (4) de $n = 4$, es decir, al tipo $(\bullet\ \bullet\ \bullet\ \bullet)$. Se tiene entonces que $c_1 = 0$, $c_2 = 0$, $c_3 = 0$, $c_4 = 1$, y la fórmula de Cauchy nos dice que hay

$$\frac{4!}{1^0 0! 2^0 0! 3^0 0! 4^1 1!} = \frac{4!}{4} = 6$$

permutaciones en S_4 del tipo $(\bullet\ \bullet\ \bullet\ \bullet)$, y éstas son:

$$(1,2,3,4); \quad (1,2,4,3); \quad (1,3,2,4); \quad (1,3,4,2); \quad (1,4,2,3); \quad (1,4,3,2).$$

Ejemplo 17. En S_4 consideremos el tipo correspondiente a la partición $(1,1,1,1)$ de $n = 4$, es decir, al tipo $(\bullet)$. Se tiene entonces que $c_1 = 4$, $c_2 = 0$, $c_3 = 0$, $c_4 = 0$, y la fórmula de Cauchy nos dice que hay

$$\frac{4!}{1^4 4! 2^0 0! 3^0 0! 4^0 0!} = \frac{4!}{4!} = 1$$

permutación en S_4 del tipo $(\bullet)$, a saber, la identidad.

La tabla siguiente resume todo lo que sabemos hasta ahora de los elementos de S_4:

Partición de 4	Tipo	Número en cada tipo	Orden del elemento	Paridad
$(1,1,1,1)$	$(\bullet)$	1	1	Par
$(1,1,2)$	$(\bullet\,\bullet)$	6	2	Impar
$(1,3)$	$(\bullet\,\bullet\,\bullet)$	8	3	Par
(4)	$(\bullet\,\bullet\,\bullet\,\bullet)$	6	4	Impar
$(2,2)$	$(\bullet\,\bullet)(\bullet\,\bullet)$	3	2	Par

En particular, el grupo alternante A_4 contiene a la identidad, los ocho 3-ciclos y los tres productos de 2-ciclos disjuntos. Explícitamente, los 12 elementos de A_4 son:

Tipo	Orden	Elementos
$(\bullet)$	1	$\mathrm{id} = (1)$
$(\bullet\,\bullet\,\bullet)$	3	$(123); (124); (132);\ (134); (142); (143); (234); (243)$
$(\bullet\,\bullet)(\bullet\,\bullet)$	2	$(12)(34);\ \ (13)(24);\ \ (14)(23)$

Usaremos los cálculos anteriores para mostrar, en el ejemplo 3 del capítulo siguiente, que A_4 es un grupo de orden 12 que no tiene un subgrupo de orden 6.

Generadores de S_n. Ya vimos en 4.5 que los ciclos generan a S_n (es decir, los elementos de S_n son productos de ciclos) y también que las transposiciones generan a S_n (4.6). A continuación veremos que S_n tiene familias de generadores más chicas, de hecho primero veremos que S_n se puede generar con dos permutaciones:

PROPOSICIÓN 4.15. *Para toda $n \geq 2$, el grupo simétrico S_n está generado por los ciclos $(12\cdots n)$ y (12).*

Demostración. Escribamos $\sigma = (12\cdots n)$ y $\tau = (12)$, y sea G el grupo generado por σ y τ. Entonces, G contiene a $\sigma\tau\sigma^{-1} = (23)$ y así G contiene a $\sigma(23)\sigma^{-1} = (34)$, y continuando este proceso vemos que G contiene a todas las transposiciones de la forma:

$$(k, k+1).$$

Entonces, G contiene a

$$\begin{aligned} (12)(23)(12) &= (13) \\ (13)(34)(13) &= (14) \\ &\vdots \\ (1,m)(m,m+1)(1,m) &= (1,m+1), \end{aligned}$$

i.e., G contiene a todas las transposiciones de la forma

$$(1, k).$$

Se sigue que G contiene a todas las transposiciones, ya que $(1,i)(1,j)(1,i) = (ij)$. Como toda permutación es producto de transposiciones, entonces $G = S_n$. □

Como consecuencia de la parte final de la demostración anterior se tiene:

COROLARIO 4.16. *Para toda $n \geq 2$, el grupo simétrico S_n está generado por las transposiciones de la forma $(1,i)$, para $i \geq 2$.* □

Otra consecuencia, de la parte media de la demostración anterior es:

COROLARIO 4.17. *Para toda $n \geq 2$, el grupo simétrico S_n está generado por las transposiciones de la forma $(i, i+1)$, para $1 \leq i \leq n-1$.* □

Ejemplo 18. Considere las permutaciones $\sigma = (1324)$ y $\tau = (12)$ de S_4 y observe que $\sigma\tau = (1324)(12) = (14)(23)$ por lo que $(\sigma\tau)^2 = 1$ y como $\sigma^4 = 1 = \tau^2$, entonces el subgrupo de S_4 generado por σ y τ es $\langle \sigma, \tau \rangle = D_8$, el grupo diédrico de orden 8.

Generadores de A_n. Los grupos A_1 y A_2 son triviales. Para $n \geq 3$ se tiene:

PROPOSICIÓN 4.18. *Para toda $n \geq 3$, el grupo alternante A_n está generado por los 3-ciclos.*

Demostración. Todo 3-ciclo se factoriza como $(a,b,c) = (a,c)(a,b)$ y por lo tanto pertenece a A_n. Probaremos ahora que toda permutación $\sigma \in A_n$ se puede factorizar como producto de 3-ciclos y para ésto basta probar que todo producto de dos transposiciones se puede escribir como el producto de 3-ciclos. Tenemos tres casos a considerar:

CASO 1. $(a,b)(c,d)$ con a,b,c,d distintos. En este caso

$$(a,b)(c,d) = (a,b,c)(b,c,d).$$

CASO 2. $(a,b)(c,a)$ con a,b,c distintos. En este caso

$$(a,b)(c,a) = (a,c,b).$$

CASO 3. $(a,b)(a,b)$ con a,b distintos. En este caso

$$(a,b)(a,b) = 1 = (a,b,c)(a,b,c)(a,b,c),$$

con c cualquier tercer elemento distinto de a y b. □

COROLARIO 4.19. *Para toda $n \geq 3$, el grupo alternante A_n está generado por los 3-ciclos de la forma*

$$(1,2,3),\ (1,2,4),\ (1,2,5),\ \ldots,\ (1,2,n).$$

Demostración. Por la proposición previa, basta probar que todo 3-ciclo (a, b, c) se puede escribir como el producto de 3-ciclos de la forma $(1, 2, i)$ con $3 \leq i \leq n$. Observemos ahora que para el 3-ciclo (a, b, c) se tiene que

$$(a, b, c) = (1, c, b)(1, a, b)(1, a, c)$$

y por lo tanto es suficiente probar que todo 3-ciclo de la forma $(1, x, y)$ se puede descomponer como producto de 3-ciclos de la forma $(1, 2, i)$ con $3 \leq i \leq n$. Se tienen tres casos:

CASO 1. $(1, x, y)$ con $x = 2$. En este caso $(1, x, y) = (1, 2, y)$ y no hay nada que probar.

CASO 2. $(1, x, y)$ con $y = 2$. En este caso

$$(1, x, y) = (1, x, 2) = (1, 2, x)(1, 2, x).$$

CASO 3. $(1, x, y)$ con $x \neq 2$ y $y \neq 2$. En este caso

$$(1, x, y) = (1, 2, y)(1, 2, y)(1, 2, x)(1, 2, y).$$

□

Notas. (1) En el siglo XIX, varios matemáticos habían estado estudiando el problema de resolver ecuaciones polinomiales (el lector seguramente conoce la fórmula para resolver ecuaciones cuadráticas y habrá oido hablar de las fórmulas para resolver ecuaciones de grados 3 y 4, que habían obtenido los matemáticos italianos Cardano y Ferrari) y la memoria de Lagrange [48] contiene lo conocido hasta su época y es el germen de lo que después conoceríamos como *Algebra moderna*. Es en este artículo donde Lagrange estudia condiciones para que una cierta ecuación algebraica, de grado n,

$$a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 = 0$$

sea soluble por radicales, considerando *permutaciones* de sus raíces $\alpha_1, \ldots, \alpha_n$ y obtiene resultados genéricos sobre estas permutaciones, incluyendo el *teorema de Lagrange* que estudiaremos en el capítulo siguiente.

(2) En la memoria [40], sobre las condiciones de solubilidad por radicales de las ecuaciones polinomiales, Galois también considera permutaciones de las raíces de los polinomios, usando la definición de permutación dada por Cauchy, pero Galois considera, por primera vez, conjuntos de substituciones *cerrados* con respecto al producto y llama *grupos* a tales conjuntos.

(3) En varios artículos publicados de 1815 a 1844, Cauchy estudia permutaciones de conjuntos finitos arbitrarios introduciendo la notación que usamos todavía, define el producto de permutaciones, permutaciones cíclicas, transposiciones, conjuntos de permutaciones generados por productos de ciertas permutaciones dadas (en particular prueba que los 3-ciclos generan todas las permutaciones pares). Como un ejemplo notamos que la *fórmula de Cauchy* la demostró en [27, pp. 192-196].

(4) La ingeniosa demostración de la invarianza, con respecto a la factorización en producto de transposiciones, de la paridad de una permutación, que dimos en este capítulo, se debe a Nelson [49].

EJERCICIO 1. Recordemos que el *signo* de una permutación $\sigma \in S_n$ está dado por

$$\operatorname{sgn}(\sigma) := \begin{cases} 1 & \text{si } \sigma \text{ es par,} \\ -1 & \text{si } \sigma \text{ es impar.} \end{cases}$$

Si $\sigma \in S_n$, una *inversión* en σ es un par de valores $\sigma(i), \sigma(j)$ tales que $i < j$ y $\sigma(i) > \sigma(j)$. Si $k(\sigma)$ es el número de inversiones en σ, demuestre que $(-1)^{k(\sigma)} = \operatorname{sgn}(\sigma)$.

EJERCICIO 2. Si G es el grupo de simetrías del triángulo equilátero, ¿puede *ver* a G como un subgrupo de un grupo simétrico? Explique y hágalo explícito. Haga lo mismo para un pentágono y un hexágono regulares.

EJERCICIO 3. Calcule los órdenes de los 6 elementos del grupo S_3.

EJERCICIO 4. Demuestre que un subconjunto $H \subseteq S_n$ es un subgrupo si y sólo si H es cerrado bajo la operación de S_n.

EJERCICIO 5. Demuestre que el orden de un k-ciclo de S_n es k.

EJERCICIO 6. Encuentre dos 2-ciclos en S_n cuyo producto sea un 3-ciclo.

EJERCICIO 7. Si $\sigma = (i_1, i_2, \ldots, i_k)$ y $\tau = (j_1, j_2, \ldots, j_t)$ son dos ciclos de S_n de longitudes k y t, respectivamente, demuestre que σ y τ son disjuntos si y sólo si $\{i_1, i_2, \ldots, i_k\} \cap \{j_1, j_2, \ldots, j_t\} = \emptyset$.

EJERCICIO 8. Si α y β son dos r-ciclos en S_n para los cuales existe un $x_0 \in \mathbb{I}_n$ tal que α y β mueven a x_0 y $\alpha^t(x_0) = \beta^t(x_0)$ para toda $t \in \mathbb{Z}$, demuestre que $\alpha = \beta$.

EJERCICIO 9. Demuestre que un k-ciclo es una permutación par si y sólo si k es impar.

EJERCICIO 10. Demuestre que los únicos elementos de orden p (un primo) de S_n son los productos de p-ciclos disjuntos.

EJERCICIO 11. Si H es un subgrupo de S_n que contiene una permutación impar, demuestre que $|H|$ es par y que la mitad de los elementos de H son permutaciones impares.

EJERCICIO 12. Para el grupo de simetrías del pentágono regular, muestre que sus 10 elementos se obtienen con las potencias r^k, para $0 \leq k < 5$ de la rotación $r = r_{2\pi/5}$

y los productos $r^k\rho$ para $0 \leq k < 5$ donde ρ es la reflexión por la recta que pasa por el vértice v_1 y el centro del pentágono. Note que sólo debe mostrar que las otras reflexiones se obtienen con los productos $r^k\rho$.

EJERCICIO 13. Mismo ejercicio para los 12 elementos del grupo de simetrías del hexágono regular.

EJERCICIO 14. Para el grupo diédrico D_{2n} de simetrías de un n-ágono regular muestre que para la rotación $r = r_{2\pi/n}$ y la reflexión ρ por la recta que pasa por el vértice v_1 y el centro del n-ágono se tienen las relaciones $r^n = e = \rho^2$ (e el neutro del grupo) y $\rho r \rho = r^{-1}$. Se sigue que D_{2n} es no abeliano.

NOTA: En los ejercicios anteriores observe que la reflexión ρ está dada por

$$\rho = \begin{pmatrix} v_1 & v_2 & v_3 & \cdots & v_{n-1} & v_n \\ v_1 & v_n & v_{n-1} & \cdots & v_3 & v_2 \end{pmatrix}$$

donde v_i denotan los vértices del n-ágono regular enumerados en sentido contrario al de las manecillas de un reloj.

EJERCICIO 15. Sea $H \subseteq D_{2n}$ el subconjunto formado por los elementos que dejan fijo al vértice v_1. Demuestre que $H = \{e, \rho\}$

EJERCICIO 16. Sea $\sigma \in D_{2n}$ cualquier elemento y suponga que σ manda el vértice v_1 en v_k para $1 \leq k \leq n$. Demuestre que $(r^{-1})^{k-1} \circ \sigma$ deja fijo a v_1 y por lo tanto $(r^{-1})^{k-1} \circ \sigma \in H$. Concluya que $\sigma = r^{k-1}$ ó $\sigma = r^{k-1}\rho$. Se sigue que todos los elementos del grupo diédrico D_{2n} son de la forma r^k con $0 \leq k < n$ ó de la forma $r^k\rho$ con $0 \leq k < n$.

EJERCICIO 17. Sean $\sigma, \tau \in S_n$. Si σ y τ son conjugados, demuestre que el número de puntos de $\mathbb{I}_n$ que σ deja fijos es igual al número de puntos fijos de τ.

EJERCICIO 18. Si $n \geq 3$, demuestre que A_n está generado por las permutaciones de la forma $(i, i+1)(j, j+1)$ para $1 \leq i, j \leq n, i \neq j \neq i+1$.

EJERCICIO 19. Si $\sigma = \kappa_1\kappa_2 \cdots \kappa_r$ es la factorización en ciclos disjuntos de una permutación $\sigma \in S_n$, y si el orden de cada ciclo κ_j es t_j, determine el orden de σ y justifique su respuesta.

EJERCICIO 20. Una permutación $\sigma \in S_n$ se dice que es un *desarrreglo* si $\sigma(i) \neq i$ para toda $i \in \mathbb{I}_n$.

- Liste los desarreglos de S_3.
- Cuente los desarreglos de S_4.
- ¿Cuántos desarreglos hay en S_n?

EJERCICIO 21. En 4.12 mostramos que las clases de conjugación de un $\sigma \in S_n$ están formadas por aquellas permutaciones que tienen la misma estructura cíclica que σ. El ejercicio siguiente nos pide determinar las clases de conjugación en el grupo alternante, de un $\sigma \in A_n$. Demuestre que:

(i) Si σ conmuta con una permutación *impar* $\tau \in S_n$, entonces la clase de conjugación de σ en A_n es igual a la clase de conjugación de σ en S_n.

(ii) Si σ no conmuta con ninguna permutación *impar* $\tau \in S_n$, entonces la clase de conjugación de σ en S_n se descompone en dos clases de conjugación en A_n, de igual tamaño y con representantes σ y $(1\ 2)\sigma(1\ 2)^{-1}$.

EJERCICIO 22. Aplique lo anterior para hallar las clases de conjugación de A_4 y A_5.

EJERCICIO 23. Sea $\sigma \in S_n$ de orden k. Si $\mathrm{mcd}(k, i) = 1$, demuestre que σ y σ^i son conjugados. Concluya que σ y σ^{-1} siempre son conjugados.

Capítulo 5

Clases laterales y grupos cociente

SI $H \subseteq G$ ES UN SUBGRUPO, podemos definir dos relaciones (que serán de equivalencia) en G:

(1) $a \equiv_i b \pmod{H} \Leftrightarrow a^{-1}b \in H$, a la que llamamos la *relación de congruencia izquierda módulo* H.

(2) $a \equiv_d b \pmod{H} \Leftrightarrow ab^{-1} \in H$, a la que llamamos la *relación de congruencia derecha módulo* H.

LEMA 5.1. *Las relaciones anteriores son de equivalencia.*

Demostración. Lo probaremos únicamente para (1). Claramente es *reflexiva* ya que $\sigma \equiv_i \sigma \pmod{H}$ porque $\sigma^{-1}\sigma = e \in H$, para toda $\sigma \in G$.

Es *simétrica*, ya que si $\sigma \equiv_i \tau \pmod{H}$ entonces $\sigma^{-1}\tau \in H$ y así $(\sigma^{-1}\tau)^{-1} \in H$. Pero, $(\sigma^{-1}\tau)^{-1} = \tau^{-1}\sigma$, y por lo tanto $\tau \equiv_i \sigma \pmod{H}$.

Es *transitiva*, ya que si $\sigma \equiv_i \tau$ y $\tau \equiv_i \vartheta$, entonces $\sigma^{-1}\tau \in H$ y $\tau^{-1}\vartheta \in H$, por lo que

$$(\sigma^{-1}\tau)(\tau^{-1}\vartheta) = \sigma^{-1}\vartheta$$

también está en H y consecuentemente $\sigma \equiv_i \vartheta$.

Para (2) es similar. □

Recordemos ahora que toda relación de equivalencia $\sim$ en un conjunto A induce una *partición* de este conjunto en *clases de equivalencia*. A la partición inducida por $\sim$ se le suele denotar por $A/\sim$ y se le llama el *conjunto cociente* de la relación. Para cada $a \in A$, la clase de equivalencia correspondiente se suele denotar por $[a]$ y es el subconjunto de A dado por

$$[a] := \{b \in A \ : \ a \sim b\}.$$

Veamos cómo son las clases de equivalencia de las relaciones de equivalencia del lema 5.1 anterior:

(1) Para la relación de congruencia izquierda módulo H, si $\sigma \in G$ es cualquier elemento, su clase de equivalencia es:

$$\begin{aligned}[\sigma] &= \{\alpha \in G : \sigma \equiv_i \alpha \ (\text{mód } H)\} \\ &= \{\alpha \in G : \sigma^{-1}\alpha \in H\} \\ &= \{\alpha \in G : \sigma^{-1}\alpha = h \text{ para algún } h \in H\} \\ &= \{\alpha \in G : \alpha = \sigma h \text{ para algún } h \in H\},\end{aligned}$$

es decir, la clase de equivalencia $[\sigma]$ de σ es el conjunto de todos los elementos de la forma σh para algún $h \in H$. Se suele denotar a esta clase de equivalencia $[\sigma]$ por σH, i.e., la clase de equivalencia de σ es el conjunto

$$\sigma H := \{\alpha \in G : \alpha = \sigma h \text{ para algún } h \in H\}.$$

A estos conjuntos se les llama las *clases laterales izquierdas* de H.

(2) Para la relación de congruencia derecha módulo H, si $\sigma \in G$ es cualquier elemento, procediendo en forma análoga al caso anterior, se muestra que su clase de equivalencia es el conjunto

$$H\sigma := \{\alpha \in G : \alpha = h\sigma \text{ para algún } h \in H\}.$$

A estos conjuntos se les llama las *clases laterales derechas* de H.

Como las clases de equivalencia de cualquier relación de equivalencia forman una partición del conjunto, se tienen las partes (1) y (2) del corolario siguiente:

COROLARIO 5.2. *Si H es un subgrupo de un grupo G, entonces:*

(1) *Las clases laterales izquierdas σH forman una partición de G.*
(2) *Las clases laterales derechas $H\sigma$ forman una partición de G.*
(3) *Existe una biyección entre el conjunto de las clases laterales izquierdas de H y el conjunto de las clases laterales derechas.*

Demostración. Sólo falta demostrar la parte (3). Para ésto, definamos la función $\Phi : \mathcal{I} \to \mathcal{D}$ entre el conjunto de clases izquierdas y el conjunto de clases derechas, mediante $\Phi(\sigma H) = H\sigma$, para cualquier $\sigma \in G$. Claramente Φ es biyectiva. □

Mostraremos ahora que todas las clases laterales (izquierdas o derechas) de un subgrupo H de G, tienen el mismo cardinal:

LEMA 5.3. *Sea $H \subseteq G$ un subgrupo. Entonces*

(1) *Las clases laterales izquierdas σH tienen el mismo cardinal que H.*

(2) *Las clases laterales derechas $H\sigma$ tienen el mismo cardinal que H.*

Demostración. (1). Para una clase lateral izquierda σH definamos la función

$$f_\sigma : \sigma H \to H$$

mediante $f_\sigma(\sigma h) := h$. Claramente f_σ es *inyectiva* ya que si $f_\sigma(\sigma h) = f_\sigma(\sigma h')$, entonces $h = h'$ y por lo tanto $\sigma h = \sigma h'$. Es *suprayectiva* ya que $h \in H$ proviene del elemento $\sigma h \in \sigma H$. Se sigue que f_σ es *biyectiva* y por lo tanto $|\sigma H| = |H|$.

Para (2) es similar. □

Ejemplo 1. Si $G = S_3$ es el grupo simétrico en 3 letras, recordemos que

$$S_3 = \{e, \sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_5\},$$

donde

$$e = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \quad \sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \quad \sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix},$$

$$\sigma_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \quad \sigma_4 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \quad \sigma_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix},$$

y si $H = \{e, \sigma_1\}$, note que $\sigma_1^2 = e$, por lo que $H \subseteq S_3$ es un subgrupo.

Las *clases laterales izquierdas* de H son:

$$\begin{aligned} eH &= H = \sigma_1 H = \{e, \sigma_1\} \\ \sigma_2 H &= \{\sigma_2, \sigma_3\} \quad \text{porque } \sigma_2\sigma_1 = \sigma_3 \\ &= \sigma_3 H \\ \sigma_4 H &= \{\sigma_4, \sigma_5\} \quad \text{porque } \sigma_4\sigma_1 = \sigma_5 \\ &= \sigma_5 H. \end{aligned}$$

Las *clases laterales derechas* de H son:

$$\begin{aligned} He &= H = H\sigma_1 = \{e, \sigma_1\} \\ H\sigma_2 &= \{\sigma_2, \sigma_4\} \quad \text{porque } \sigma_1\sigma_2 = \sigma_4 \\ &= H\sigma_4 \\ H\sigma_3 &= \{\sigma_3, \sigma_5\} \quad \text{porque } \sigma_1\sigma_3 = \sigma_5 \\ &= H\sigma_5. \end{aligned}$$

Note que, excepto por la clase lateral de la identidad $eH = H = He$, en este ejemplo las clases laterales izquierdas y derechas son *diferentes*, i.e., en general,

$$\sigma H \neq H\sigma.$$

Ejemplo 2. Si $G = (\mathbb{Z}, +)$ es el grupo aditivo de los enteros y si $H = n\mathbb{Z}$ es el subgrupo de múltiplos de un entero fijo $n \geq 1$, como $G = (\mathbb{Z}, +)$ es un *grupo abeliano*

toda clase lateral izquierda es una clase lateral derecha. Las clases laterales (izquierdas o derechas) de $n\mathbb{Z}$ en $\mathbb{Z}$ están dadas como sigue: para $k \in \mathbb{Z}$, si dividimos k entre $n \geq 1$:

$$k = nq + r \quad \text{con } 0 \leq r < n,$$

se tiene que $k \equiv r \pmod{n\mathbb{Z}}$ ya que $k - r = nq \in n\mathbb{Z}$. Se sigue que la clase lateral de k es igual a la clase lateral de r y como las posibilidades para el residuo r son

$$r = 0, 1, 2, 3, \ldots, n-1$$

entonces hay (a lo más) n clases laterales dadas por

$$\begin{aligned} r + n\mathbb{Z} &:= \{r + h \,:\, h \in n\mathbb{Z}\} = \{r + h \,:\, h = nt \ \text{ con } t \in \mathbb{Z}\} \\ &= \{r + nt \,:\, \text{con } t \in \mathbb{Z}\}, \end{aligned}$$

para $0 \leq r \leq n-1$. Observemos ahora que, si $0 \leq r, r' \leq n-1$, y si sucediera que las clases de r y r' fueran iguales, $r + n\mathbb{Z} = r' + n\mathbb{Z}$, entonces $r \equiv r' \pmod{n\mathbb{Z}}$ y por lo tanto se tendría que $r - r' \in n\mathbb{Z}$, i.e., n divide a $r - r'$. Sin perder generalidad podemos suponer que $r \geq r'$, y así se tendría que $0 \leq r - r' < n$ y además n divide a $r - r'$. Como este número es *menor* que n, esto sólo puede suceder si $r - r' = 0$, i.e., si $r = r'$. Hemos así probado que las clases laterales correspondientes a los n valores de r entre 0 y $n-1$, son distintas. Es decir, las clases laterales de $n\mathbb{Z}$ en $\mathbb{Z}$ son

$$n\mathbb{Z}, 1 + n\mathbb{Z}, 2 + n\mathbb{Z}, 3 + n\mathbb{Z}, \ldots, (n-1) + n\mathbb{Z}.$$

Si $H \subseteq G$ es un subgrupo de un grupo *finito* G, es obvio que $|H| \leq |G|$. El teorema siguiente mejora substancialmente esta observación y es el primer teorema importante en el estudio de los grupos finitos. Para su demostración usaremos lo que hemos visto de clases laterales (digamos, izquierdas):

TEOREMA 5.4 (Lagrange). *Sea G un grupo finito de orden n y sea $H \subseteq G$ un subgrupo. Entonces, el orden de H divide al orden de G.*

Demostración. Sea $k = |H|$ el orden de H. Consideremos la colección de todas las clases laterales izquierdas σH de H en G. Como G es finito es claro que sólo hay un número finito de clases laterales izquierdas; sea q el número de clases laterales izquierdas de H en G y sean

$$\sigma_1 H, \sigma_2 H, \ldots, \sigma_q H$$

todas estas q clases laterales. Por el corolario 5.2 estas clases forman una partición de G, en particular son disjuntas por pares y su unión es todo G. Se sigue que

$$n = |G| = \sum_{j=1}^{q} |\sigma_j H|.$$

Ahora, por el lema 5.3, todas las clases laterales $\sigma_i H$ tienen el mismo cardinal que H, i.e., $|\sigma_j H| = |H| = k$. Substituyendo ésto en la igualdad anterior se sigue que:

$$n = |G| = \sum_{j=1}^{q} |\sigma_j H| = \sum_{j=1}^{q} |H| = \sum_{j=1}^{q} k = kq,$$

y por lo tanto k divide a n, como se quería. □

Si G es un grupo y $H \subseteq G$ es un subgrupo, al cardinal del conjunto de clases laterales (digamos, izquierdas) de H en G se le llama el *índice* de H en G y se denota $[G : H]$. El teorema de Lagrange nos dice que si G es finito, entonces $|G| = |H|[G : H]$.

COROLARIO 5.5. *Si G es un grupo finito y $\sigma \in G$ es cualquier elemento, entonces el orden de σ divide al orden de G.*

Demostración. El orden de un elemento σ es el orden del subgrupo cíclico $\langle\sigma\rangle$ generado por σ y por el teorema de Lagrange el orden del subgrupo $\langle\sigma\rangle$ divide al orden de G. □

COROLARIO 5.6. *Si G es un grupo finito de orden n y $\sigma \in G$ es cualquier elemento, entonces $\sigma^n = e$.*

Demostración. Sea k el orden de σ. Por el corolario anterior $n = kq$ con $q \in \mathbb{Z}$. Se tiene así que $\sigma^n = \sigma^{kq} = (\sigma^k)^q = e^q = e$. □

COROLARIO 5.7. *Todo grupo finito de orden primo es cíclico.*

Demostración. Si $|G| = p$ es primo, sea $\sigma \neq e$ en G. Por el teorema de Lagrange, el orden del subgrupo cíclico $\langle\sigma\rangle$ divide al orden de G, i.e., divide a p y por lo tanto $|\langle\sigma\rangle| = p$ ó 1, ya que p es primo. Ahora, como $\langle\sigma\rangle$ contiene a $\sigma \neq e$, entonces su orden no puede ser 1. Se sigue que $|\langle\sigma\rangle| = p$, i.e., $\langle\sigma\rangle$ es un subgrupo de G de orden igual al orden de G, y por lo tanto debe ser igual a G, i.e., $G = \langle\sigma\rangle$, i.e., G es cíclico. □

Observe cómo el corolario anterior es un resultado genérico, en el sentido que nos dice cómo es un grupo finito de cierto tipo (cíclico, en este caso) conociendo cómo es su orden (primo, en este caso), y además fue una consecuencia directa del teorema de Lagrange.

También, dado un grupo finito arbitrario, si queremos listar todos sus subgrupos, gracias al teorema de Lagrange sólo tenemos que buscar en aquellos órdenes que sean divisores del orden del grupo G dado. Por ejemplo, si G tiene orden 10, sólo puede tener subgrupos de orden 1, 2, 5 y 10. Esto simplifica bastante el proceso de obtener la red de subgrupos de un grupo finito dado.

Podría uno preguntarse si el *recíproco* del teorema de Lagrange es verdadero, es decir, si G es un grupo finito de orden n y si k es un entero que divide a n (decimos que k es un divisor de n) nos preguntamos si siempre existe un subgrupo H de G de

orden k. Esto es cierto para grupos abelianos finitos, pero para grupos no abelianos es falso en general:

Ejemplo 3. El grupo alternante A_4 (que tiene orden 12) no tiene subgrupos de orden 6. Una demostración de este hecho la daremos al final del capítulo.

Se puede decir que el resto del libro será la búsqueda de un *recíproco parcial* del teorema de Lagrange, es decir, tratar de responder a la pregunta: ¿para qué divisores del orden de un grupo finito se tienen subgrupos cuyo orden sea el divisor dado?

El grupo cociente. Si A y B son dos *subconjuntos* de un grupo G y si definimos

$$AB := \{ab \ : \ a \in A \ \text{ y } \ b \in B\},$$

entonces AB es un subconjunto de G. Note que la asociatividad del producto del grupo G implica que el producto de subconjuntos de G es *asociativo*, i.e.,

$$A(BC) = (AB)C.$$

Observe ahora que si $A = \{a\} \subseteq G$ y $B = H$ es un subgrupo de G, entonces

$$AB = \{a\}H = aH \quad \text{y} \quad BA = H\{a\} = Ha$$

son las clases laterales izquierdas y derechas de H en G que definimos previamente.

También, si $A = H = B$ es un subgrupo de G, entonces

$$HH = H$$

ya que $HH = \{hh' \ : \ h \in H, h' \in H\} \subseteq H$ porque H es cerrado bajo productos por ser un subgrupo. Por otra parte, si $h \in H$, entonces $h = he \in HH$ con $h \in H$ y $e \in H$, y por lo tanto $H \subseteq HH$. Se sigue que $H = HH$ como se quería.

Si H es un subgrupo de un grupo G y denotamos al conjunto de clases laterales izquierdas σH de H en G por G/H, es natural que pensemos en cómo darle al conjunto G/H una estructura de grupo que sea heredada, de alguna forma, de la estructura de grupo de G. Así, dadas dos clases laterales izquierdas σH y τH queremos multiplicarlas para obtener otra clase lateral izquierda, digamos

$$(\sigma H)(\tau H) = \vartheta H.$$

Ahora, como cada clase lateral gH es un subconjunto de G:

$$gH = \{gh \ : \ h \in H\}$$

si queremos multiplicar σH por τH es natural que la multiplicación sea la multiplicación de los conjuntos σH y τH como la definimos arriba. Observemos ahora que el producto de estos dos conjuntos es el conjunto

$$(\sigma H)(\tau H) = \{(\sigma h)(\tau h') \ : \ h, h' \in H\}$$

y como queremos que este conjunto sea otra clase lateral izquierda de H en G, digamos ϑH, i.e., queremos que

$$(\sigma H)(\tau H) = \vartheta H$$

observemos que como $\sigma\tau = (\sigma e)(\tau e) \in (\sigma H)(\tau H)$, entonces $\sigma\tau$ debe ser un elemento de ϑH y, ya que las clases laterales izquierdas de H son disjuntas, entonces $\vartheta H = (\sigma\tau)H$ y por lo tanto se debe tener que

$$(\sigma H)(\tau H) = (\sigma\tau)H.$$

Recordemos ahora que la igualdad anterior quiere decir que el producto de todos los elementos del conjunto σH por todos los elementos del conjunto τH es igual al conjunto $(\sigma\tau)H$. ¡Son demasiados productos para obtener una sóla clase lateral! Así, en lugar de considerar *todos* los elementos de cada clase lateral αH la idea es elegir algunos de ellos que represente a los otros (como en un parlamento democrático). Al elegir un elemento αh en la clase lateral αH, llamaremos al elemento αh un *representante* de la clase lateral αH. Desde el punto de vista democrático, cualquier elemento de la clase lateral αH puede ser elegido representante de la clase. Entonces, la idea para definir el producto de dos clases laterales izquierdas σH y τH es elegir representantes de cada una de las clases, digamos σh y $\tau h'$, y multiplicar estos representantes en G para obtener $(\sigma h)(\tau h') \in G$ y luego considerar su clase lateral izquierda $(\sigma h)(\tau h')H$, para *definir*

$$(\sigma H)(\tau H) := (\sigma h)(\tau h')H.$$

¿Qué quiere decir la igualdad anterior? El significado que queremos darle es que la igualdad diga que los productos de *cualesquiera representantes* de σH por cualesquiera representantes de τH están en la misma clase lateral izquierda, i.e., si $\sigma h, \sigma h_1$ son dos representantes de σH y si $\tau h', \tau h_1'$ son representantes de τH, queremos que

$$(\sigma h)(\tau h') \equiv_i (\sigma h_1)(\tau h_1') \ (\text{mód } H),$$

i.e., que la operación que queremos definir *no dependa de la elección de los representantes* de las clases laterales σH y τH. Si esto sucede, diremos que la operación *está bien definida* en el *conjunto cociente* G/H. Lo primero que deseamos entonces es encontrar condiciones en el subgrupo H y el grupo G para que lo anterior suceda, pero antes, supongamos por un momento que la operación anterior en G/H está bien definida. Mostraremos que G/H tiene una estructura de grupo heredada de la estructura de grupo de G:

LEMA 5.8. *Sea H un subgrupo de un grupo G y supongamos que la operación anterior en G/H está bien definida. Entonces, G/H es un grupo bajo esta operación y se le llama el* grupo cociente *de G por H.*

Demostración. Si $\sigma H, \tau H$ y ϑH son tres clases laterales izquierdas de H en G, como observamos antes que el producto de subconjuntos de G es asociativo, entonces en

particular el producto de clases laterales de G/H es asociativo. Para otra demostración de la asociatividad del producto:

$$\sigma H(\tau H\vartheta H) = (\sigma H\tau H)\vartheta H,$$

como por hipótesis el producto en G/H está bien definido, i.e., no depende de los representantes de las clases involucradas, entonces, por ejemplo, para multiplicar $\tau H\vartheta H$, eligiendo como representantes de las clases correspondientes a $\tau \in \tau H$ y a $\vartheta \in \vartheta H$ se tiene que

$$\tau H\vartheta H = (\tau\vartheta)H$$

y así eligiendo σ como representante de σH, se tiene que:

$$\begin{aligned} \sigma H(\tau H\vartheta H) &= \sigma H(\tau\vartheta)H = (\sigma(\tau\vartheta))H \\ (\sigma H\tau H)\vartheta H &= ((\sigma\tau)H)\vartheta H = ((\sigma\tau)\vartheta)H \end{aligned}$$

y como $\sigma(\tau\vartheta) = (\sigma\tau)\vartheta$ por la asociatividad del producto en G, entonces los términos de la derecha de las dos igualdades anteriores son el mismo y por lo tanto

$$\sigma H(\tau H\vartheta H) = (\sigma H\tau H)\vartheta H.$$

La clase lateral izquierda $eH = H$ es el neutro para la operación en G/H ya que

$$\sigma HeH = (\sigma e)H = \sigma H.$$

Finalmente, si $\sigma H \in G/H$, su inverso es $\sigma^{-1}H$ ya que

$$\sigma H\sigma^{-1}H = (\sigma\sigma^{-1})H = eH = H.$$

□

El lema anterior nos dice que las propiedades de la operación de grupo de G se heredan al producto G/H una vez que la operación de multiplicación de clases laterales izquierdas esté bien definida. El teorema siguiente nos dice cuándo sucede esto:

TEOREMA 5.9. *Sea H un subgrupo de un grupo G. La multiplicación anterior de clases laterales izquierdas en G/H está bien definida si y sólo si toda clase lateral izquierda de H es una clase lateral derecha de H en G. Es decir, si y sólo si $\sigma H = H\sigma$, para todo $\sigma \in H$.*

Demostración. Antes de comenzar aclaremos lo que significa la última frase del teorema: *toda clase lateral izquierda σH es una clase lateral derecha es equivalente a decir que $\sigma H = H\sigma$*. Para probar ésto observemos que si σH es igual a la clase lateral derecha $H\tau$, como $\sigma = \sigma e \in \sigma H = H\tau$, entonces $\sigma \in H\tau$ y como las clases laterales derechas forman una partición de G, entonces $H\tau = H\sigma$, es decir, $\sigma H = H\sigma$. También observamos que dos clases laterales izquierdas aH, bH son iguales, $aH = bH$ si y sólo si $b^{-1}a \in H$. Una vez aclarado ésto, podemos proceder con la demostración del teorema:

Supongamos primero que toda clase lateral izquierda es una clase lateral derecha, i.e., $bH = Hb$ para cualquier $b \in G$. Dadas aH y bH en G/H, escojamos representantes $a, ah \in aH$ y $b, bh' \in bH$. Queremos probar que $(ab)H = (ahbh')H$, i.e., queremos probar que $(ab)(ahbh')^{-1} \in H$. Ahora,

$$\begin{aligned}
(ab)(ahbh')^{-1} &= abh'^{-1}b^{-1}h^{-1}a^{-1} \\
&= abb^{-1}kh^{-1}a^{-1} \quad \text{ya que } h'^{-1}b^{-1} \in Hb^{-1} = b^{-1}H \\
&\qquad\qquad \text{y así } h'^{-1}b^{-1} = b^{-1}k \text{ para algún } k \in H \\
&= ak'a^{-1} \qquad (\text{para } k' = kh^{-1} \in H) \\
&= aa^{-1}k'' \qquad \text{ya que } k'a^{-1} \in Ha^{-1} = a^{-1}H \\
&\qquad\qquad \text{y así } k'a^{-1} = a^{-1}k'' \text{ para algún } k'' \in H \\
&= k'' \in H,
\end{aligned}$$

como se quería.

Supongamos ahora que el producto de dos clases laterales izquierdas es de nuevo una clase lateral izquierda y que no depende de la elección de los representantes de cada clase lateral. Mostraremos entonces que $aH = Ha$ para todo $a \in G$. En efecto, como observamos previamente, si aH y bH son dos clases laterales izquierdas arbitrarias, entonces $(aH)(bH) = (ab)H$. En particular, para $b = a^{-1}$ se tiene que

$$(aH)(a^{-1}H) = (aa^{-1})H = H \tag{1}$$

y por lo tanto

$$aHa^{-1} = (aHa^{-1})e \subseteq aHa^{-1}H = H \quad \text{por (1)},$$

y por lo tanto

$$aHa^{-1} \subseteq H. \tag{2}$$

Por otra parte, si $h \in H$ es cualquier elemento, entonces por (2) se tiene que $bhb^{-1} \in H$ para cualquier $b \in G$. En particular, para $b = a^{-1}$ se tiene que $a^{-1}ha \in H$ ya que $(a^{-1})^{-1} = a$. Ahora, $a^{-1}ha \in H$ quiere decir que $a^{-1}ha = h'$, para algún $h' \in H$, y como $ah'a^{-1} \in H$ por (2), entonces

$$h = a(a^{-1}ha)a^{-1} = ah'a^{-1} \in aHa^{-1},$$

y por lo tanto

$$H \subseteq aHa^{-1}. \tag{3}$$

De (2) y (3) se sigue que

$$H = aHa^{-1} \quad \text{para toda } a \in G. \tag{4}$$

De esta igualdad, multiplicando por a a la derecha, se sigue que $Ha = aH$ como se quería. □

Hemos visto que, en general, si G es un grupo y H es un subgrupo, las clases laterales izquierdas no son iguales a las clases laterales derechas, i.e.,

$$\sigma H \neq H\sigma, \quad \text{en general,}$$

por ejemplo, para $G = S_3$, vimos en el ejemplo 1 que si $H = \{e, \sigma_1\}$ se tiene que $\sigma_2 H \neq H\sigma_2$.

Así que no siempre el conjunto G/H es un grupo bajo la operación anterior heredada de la estructura de grupo de G.

Vimos en la demostración del teorema anterior que la igualdad $H = aHa^{-1}$ se sigue formalmente de la inclusión $aHa^{-1} \subseteq H$. Por otra parte, por definición de igualdad, $H = aHa^{-1}$ implica la inclusión $aHa^{-1} \subseteq H$. Finalmente, también vimos en la parte final de la demostración del teorema anterior que la igualdad $H = aHa^{-1}$ implica que $aH = Ha$. Esto lo resumimos en:

COROLARIO 5.10. *Sea H un subgrupo de G. Las afirmaciones siguientes son equivalentes:*

(1) $aHa^{-1} \subseteq H$, *para toda* $a \in G$.
(2) $aHa^{-1} = H$, *para toda* $a \in G$.
(3) $aH = Ha$, *para toda* $a \in G$.

□

Subgrupos normales. Cuando un subgrupo H de G satisface cualquiera de las tres condiciones del corolario anterior, diremos que H es un *subgrupo normal* de G y lo denotamos mediante:

$$H \lhd G.$$

Así, por el lema 5.8, el conjunto G/H resulta un grupo al que llamaremos el *grupo cociente* de G por H.

Ejemplo 4. Por supuesto que la igualdad $\sigma H = H\sigma$ se tiene si G es *abeliano*, es decir todos los subgrupos de un grupo abeliano son normales.

Ejemplo 5. Si $G = S_3 = \{e, \sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_5\}$ (para la notación, vea el ejemplo 3 de §4) y $A_3 = \{2, \sigma_3, \sigma_4\}$, entonces $A_3 \lhd S_3$, ya que calculando los productos:

$$\sigma_1\sigma_3 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = \sigma_5$$

$$\sigma_1\sigma_4 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \sigma_2$$

$$\sigma_2\sigma_3 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \sigma_1$$

$$\sigma_2\sigma_4 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = \sigma_5$$

$$\sigma_5\sigma_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \sigma_2$$

$$\sigma_5\sigma_4 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \sigma_1$$

se tiene que sus clases laterales izquierdas son:

$$eA_3 = \{2, \sigma_3, \sigma_4\}$$
$$\sigma_1 A_3 = \{\sigma_1, \sigma_2, \sigma_5\}.$$

En forma similar se calculan las clases laterales derechas:

$$A_3 e = \{2, \sigma_3, \sigma_4\}$$
$$A_3\sigma_1 = \{\sigma_1, \sigma_2, \sigma_5\},$$

y por lo tanto $eA_3 = A_3 = A_3 e$ y $\sigma_1 A_3 = A_3\sigma_1$. Se sigue que el grupo cociente S_3/A_3 es:

$$S_3/A_3 = \{A_3, \sigma_1 A_3\}.$$

Ejemplo 6. Si G es cualquier grupo, el subgrupo trivial $\{e\} \subseteq G$ es normal, ya que para toda $\sigma \in G$ se tiene que

$$\sigma e \sigma^{-1} = \sigma\sigma^{-1} = e \in \{e\}.$$

Ejemplo 7. Si G es cualquier grupo, el subgrupo total $G \subseteq G$ es normal, ya que para toda $\sigma \in G$ y toda $a \in G$ se tiene que

$$\sigma a \sigma^{-1} \in G.$$

Ejemplo 8. Si $G = (\mathbb{Z}, +)$ es el grupo aditivo de los enteros y $N = n\mathbb{Z}$ es el subgrupo de los enteros múltiplos de n, como G es abeliano entonces $n\mathbb{Z} \lhd \mathbb{Z}$. El grupo cociente es el grupo aditivo de clases residuales módulo n:

$$\mathbb{Z}/n\mathbb{Z} = \{[0], [1], [2], [3], \ldots, [n-1]\}.$$

Ejemplo 9. Sea $G = \mathrm{GL}(n, \mathbb{R})$ el grupo de matrices invertibles $n \times n$ con entradas reales, i.e., cuyo determinante es $\neq 0$. Sea $H = \mathrm{SL}(n, \mathbb{R})$ el subconjunto de G formado por las matrices cuyo determinantes es $= 1$. Entonces, $H \lhd G$ ya que, claramente es subgrupo y es normal porque si $A \in H$ y $B \in G$, entonces $\det A = 1$ y como el determinante de un producto de matrices es el producto de los determinantes,

$$\det(BAB^{-1}) = \det B \det A \det(B^{-1}) = (\det B)(1)(\det B)^{-1} = 1$$

(donde usamos que $\det(B^{-1}) = (\det B)^{-1}$) y por lo tanto $BAB^{-1} \in H$.

Ejemplo 10. El subgrupo alternante A_n es un subgrupo normal de S_n, ya que si $\sigma \in A_n$ y $\tau \in S_n$ entonces τ y τ^{-1} tienen la misma paridad y como σ es par, entonces $\tau\sigma\tau^{-1}$ es par, i.e., está en A_n.

Ejemplo 11. Si G es un grupo cíclico, ya vimos que los subgrupos de G también son cíclicos. Ahora, como G es abeliano, todos sus subgrupos son normales y así podemos considerar los cocientes G/H (que también son abelianos) y se tiene que:

PROPOSICIÓN 5.11. *Si G es un grupo cíclico y $H \subseteq G$ es un subgrupo, entonces G/H también es cíclico.*

Demostración. Escribamos $G = \langle\sigma\rangle$ con σ un generador de G. Sea $H \subseteq G$ un subgrupo cualquiera. Mostraremos que la clase lateral σH (del generador σ de G) *genera* al cociente G/H. En efecto, si τH es cualquier elemento de G/H, entonces $\tau \in G = \langle\sigma\rangle$ y así existe un entero $n \in \mathbb{Z}$ tal que $\sigma^n = \tau$, por lo que $\tau H = \sigma^n H = (\sigma H)^n$ y por lo tanto σH genera a G/H. □

Ejemplo 12. Es importante observar que *la normalidad no es transitiva*, es decir, aun cuando se tenga que $K \lhd H \lhd G$, no se puede concluir que $K \lhd G$ en general. Un contraejemplo es el siguiente: sea $G = A_4$ y sea $H = \{1, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$. Es fácil ver que $H \lhd G$ y que H es abeliano. H se conoce como el *grupo de Klein de 4 elementos*. Sea $K = \{1, (1\ 2)(3\ 4)\}$. Como $[(1\ 2)(3\ 4)]^2 = (1\ 2)^2(3\ 4)^2 = 1$, entonces K es un subgrupo de H y $K \lhd H$. Sin embargo, K no es normal en G ya que para el elemento $\tau = (1\ 2)(3\ 4) \in K$ y para $\sigma = (1\ 2\ 3) \in G = A_4$, el conjugado

$$\sigma\tau\sigma^{-1} = \sigma(1\ 2)(3\ 4)\sigma^{-1} = (\sigma(1)\ \sigma(2))(\sigma(3)\ \sigma(4)) = (2\ 3)(1\ 4) \notin K.$$

Subgrupos de un cociente. Si $N \lhd G$ el resultado siguiente nos dice que hay una correspondencia biyectiva entre los subgrupos de G/N y ciertos subgrupos del grupo G:

TEOREMA 5.12 (Teorema de correspondencia). *Si N es un subgrupo normal de G, entonces existe una biyección entre la familia de subgrupos de G/N y los subgrupos $H \subseteq G$ tales que $N \subseteq H$. La correspondencia es*

$$H \subseteq G \text{ tal que } N \subseteq H \mapsto H/N \subseteq G/N.$$

Demostración. Sea H un subgrupo de G tal que $N \subseteq H$. Entonces, el subconjunto

$$H/N := \{hN \ : \ h \in H\} \subseteq G/N$$

es un subgrupo de G/N ya que $e \in H$ por lo que $eN \in H/N$. Supongamos ahora que aN, bN son dos elementos de H/N, i.e., $a, b \in H$. Entonces, $ab \in H$ por lo que $abN \in H/N$. Finalmente, si $aN \in H/N$, i.e., si $a \in H$, entonces $a^{-1} \in H$ por lo que $a^{-1}N \in H/N$.

Mostraremos ahora que la correspondencia anterior es *inyectiva*. En efecto, si H, H' son dos subgrupos de G tales que $N \subseteq H$ y $N \subseteq H'$ y satisfacen que $H/N = H'/N$, probaremos que $H = H'$. Para esto, observemos que si $h \in H$, entonces $hN \in H/N = H'/N$, por lo que $hN \in H'/N$ y así $hN = \bar{h}N$ con $\bar{h} \in H'$. Se sigue que $h = he = \bar{h}n$ para algún $n \in N$; y como $N \subseteq H'$, entonces $\bar{h}n \in H'$ y por lo tanto $h \in H'$. Hemos así mostrado que $H \subseteq H'$. En forma similar se muestra que $H' \subseteq H$.

Mostraremos ahora que la correspondencia anterior es *suprayectiva*. En efecto, si $\mathcal{H} \subseteq G/N$ es cualquier subgrupo, sea $H := \{h \in H \ : \ hN \in \mathcal{H}\}$. Entonces,

(i) H es un subgrupo de G ya que:

- $e \in H$ porque $eN \in \mathcal{H}$ (es el neutro de G/N).
- Si $a, b \in H$, entonces $aN, bN \in \mathcal{H}$ y así $(aN)(bN) = (ab)N \in \mathcal{H}$ por lo que $ab \in H$.
- Si $a \in H$, entonces $aN \in \mathcal{H}$ y así $(aN)^{-1} = a^{-1}N \in \mathcal{H}$ por lo que $a^{-1} \in H$.

(ii) $H \supseteq N$, ya que si $a \in N$, entonces $aN = N = eN \in \mathcal{H}$ por lo que $a \in H$.

(iii) $\mathcal{H} = H/N$ ya que:

- Si $aN \in \mathcal{H}$, entonces $a \in H$ por definición de H y así $aN \in H/N$.
- Si $hN \in H/N$, i.e., si $h \in H$, entonces $hN \in \mathcal{H}$ por definición de H.

□

Un contraejemplo al recíproco del teorema de Lagrange. A continuación damos la demostración, prometida en el ejemplo 3, de que *el grupo alternante* A_4 (que tiene orden 12) *no tiene subgrupos de orden* 6.

En efecto[1], supongamos que existe un subgrupo $H \subseteq A_4$ de orden 6. Como vimos después del ejemplo 17 en el capítulo 4, el grupo A_4 tiene 8 elementos de orden 3. Si $\alpha \in A_4$ es cualquier elemento de orden 3, como el índice de H en A_4 es 2, entonces a lo más dos de las clases laterales $H, \alpha H, \alpha^2 H$ pueden ser distintas. Observemos ahora que la igualdad de cualesquiera dos de estas clases implica que $\alpha \in H$, ya que para $H = \alpha H$ es obvio; para $\alpha H = \alpha^2 H$ multiplicando a la izquierda por α^{-1} se tiene que $H = \alpha H$ y estamos en el primer caso; para $H = \alpha^2 H$, multiplicando por α a la izquierda se tiene que $\alpha H = \alpha^3 H = H$ ya que α es de orden 3 y así, de nuevo estamos en el primer caso. Se sigue que H contiene a todos los 8 elementos de orden 3 de A_4, en contradicción con $|H| = 6$.

Conmutadores. Si G es un grupo y si $a, b \in G$, el *conmutador* de a y b, denotado por $[a, b]$ es el elemento

$$[a, b] := aba^{-1}b^{-1} \in G.$$

En general, el producto de dos conmutadores no tiene por qué ser un conmutador, aunque es un poco latoso encontrar un ejemplo[2]. Denotemos por $[G, G]$ al subgrupo de G generado por todos los conmutadores $[a, b]$ con $a, b \in G$. Al grupo $[G, G]$ se le llama el *subgrupo conmutador* de G.

LEMA 5.13. $[G, G] \lhd G$.

Demostración. Los elementos de $[G, G]$ son productos finitos de la forma

$$(*) \qquad x = [a_1, b_1] \cdots [a_t, b_t] = a_1 b_1 a_1^{-1} b_1^{-1} \cdots a_t b_t a_t^{-1} b_t^{-1}$$

y para cada uno de los factores de la forma $[a, b]$, para cualquier $g \in G$ se tiene que:

$$g[a, b]g^{-1} = gaba^{-1}b^{-1}g^{-1} = gag^{-1}gbg^{-1}ga^{-1}g^{-1}gb^{-1}g^{-1} = [gag^{-1}, gbg^{-1}],$$

el cual es un elemento de $[G, G]$, y el paso al caso general $(*)$ es directo. □

Conmutadores en S_n y A_n. En el caso cuando $G = S_n$ observemos que los conmutadores $[\sigma, \tau]$ con $\sigma, \tau \in S_n$, son permutaciones pares ya que σ y σ^{-1} (respectivamente, τ y τ^{-1}) tienen la misma paridad. Se sigue que

$$[A_n, A_n] \subseteq [S_n, S_n] \subseteq A_n$$

para toda $n \geq 1$.

PROPOSICIÓN 5.14. (1) *Si* $n \geq 3$, *entonces* $[S_n, S_n] = A_n$.

(2) *Si* $n \geq 5$, *entonces* $[A_n, A_n] = A_n$.

---

[1] Esta demostración es de J. A. Gallian, Amer. Math. Monthly **66** (1993), p. 23.

[2] Para un ejemplo, en S_{16}, véase el ejercicio 19 tomado de [4, página 39].

Demostración. (1) Como en general $[S_n, S_n] \subseteq A_n$, entonces es suficiente probar que $A_n \subseteq [S_n, S_n]$. Ahora, como $n \geq 3$, por 4.18 el grupo A_n está generado por los 3-ciclos y así basta entonces probar que todo 3-ciclo (a, b, c) está en $[S_n, S_n]$. Para ésto observemos que

$$(a, b, c) = (a, b)(a, c)(a, b)(a, c) = (a, b)(a, c)(a, b)^{-1}(a, c)^{-1} \in [S_n, S_n]$$

ya que la inversa de una transposición es ella misma.

(2) Como en general $[A_n, A_n] \subseteq A_n$, entonces es suficiente probar que $A_n \subseteq [A_n, A_n]$ y para ésto basta probar que todo 3-ciclo (a, b, c) está en $[A_n, A_n]$. Ahora, como $n \geq 5$, entonces existen $e, f \in \mathbb{I}_n$ diferentes de a, b, c, y se tiene que

$$(a, b, c) = [(d, c, a), (a, e, d)][(a, e, d), (d, b, a)].$$

□

Notas. La noción de *subgrupo normal* la introdujo Galois en [40]. El concepto de *grupo cociente* fue introducido, en 1889, por Otto Hölder [42]; previamente sólo había sido reconocido explícitamente el *índice* de un subgrupo de un grupo finito, por ejemplo por Camille Jordan en [11] o como grupos de Galois de la ecuación auxiliar o resolvente de un polinomio dado. Para los antecedentes del teorema de Lagrange, vea las notas al final del capítulo 8.

EJERCICIO 1. En el teorema de correspondencia, si $N \lhd G$ y si $H \subseteq G$ es un subgrupo que contiene a N, denotando con $\overline{H}$ a su imagen en $\overline{G} = G/N$, demuestre que $H \lhd G$ si y sólo si $\overline{H} \lhd \overline{G}$.

EJERCICIO 2. Si G es cualquier grupo y H es un subgrupo de índice 2, demuestre que $H \lhd G$.

EJERCICIO 3. Si G es un grupo, sea $Z(G)$ el centro de G (vea el ejercicio 7 del capítulo 2).

(i) Demuestre que $Z(G) \lhd G$.
(ii) Demuestre que si $G/Z(G)$ es cíclico, entonces G es abeliano.

EJERCICIO 4. Si H y K son subgrupos normales de G, demuestre que $H \cap K$ es normal en G.

EJERCICIO 5. Si $H \subseteq G$ es un subgrupo arbitrario y $N \lhd G$, demuestre que NH es un subgrupo de G.

EJERCICIO 6. Si $H \lhd G$ y $K \lhd G$, demuestre que $HK \lhd G$.

EJERCICIO 7. Si G es cualquier grupo y $K \subseteq G$ es un subgrupo cíclico, demuestre que todo subgrupo de K es normal en G.

EJERCICIO 8. Demuestre que el único subgrupo de orden 12 de S_4 es A_4.

EJERCICIO 9. Si D_{2n} es el grupo diédrico y $R_n \subseteq D_{2n}$ es el subgrupo de las rotaciones, demuestre que $R_n \lhd D_{2n}$.

EJERCICIO 10. Si G es un grupo y $a, b \in G$, demuestre que:

(1) $[a,b]^{-1} = [b,a]$

(2) $[a,b]^{-1} = [a^{-1},b]$

(3) $[a,b]^n = [a^n,b]$, para todo $n \in \mathbb{Z}$.

EJERCICIO 11. Sea G cualquier grupo y sea $H \lhd G$. Demuestre que G/H es abeliano si y sólo si $[G,G] \subseteq H$.

EJERCICIO 12. En particular, $G/[G,G]$ es abeliano y se llama la *abelianización* del grupo G. Pruebe que $G/[G,G]$ es el mayor cociente abeliano de G.

EJERCICIO 13. Sea G un grupo finito de orden impar. Si x es el producto de todos los elementos de G, en cualquier orden, demuestre que $x \in [G,G]$.

EJERCICIO 14. Muestre que

$$[A_4, A_4] = \{1, (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)\},$$

por lo que $[A_4, A_4] \subsetneq A_4$.

EJERCICIO 15. Si $G = \mathrm{GL}(n,\mathbb{R})$ y si $H = \mathrm{SL}(n,\mathbb{R})$, vea el ejemplo 9, dada una matriz $A \in \mathrm{GL}(n,\mathbb{R})$ demuestre que su clase lateral es

$$AH = A \cdot \mathrm{SL}(n,\mathbb{R}) = \{M \in \mathrm{GL}(n,\mathbb{R}) \ : \ \det M = \det A\}.$$

EJERCICIO 16. ¿Puedes describir al grupo cociente $\mathrm{GL}(n,\mathbb{R})/\mathrm{SL}(n,\mathbb{R})$ del ejemplo 9?

EJERCICIO 17. Otra demostración de que A_4 no tiene un subgrupo de orden 6. Suponga que $H \subseteq A_4$ es un subgrupo tal que $|H| = 6$:

(i) Concluya que $H \lhd A_4$.

(ii) Por (i), A_4/H es un grupo. Demuestre que esto implica que para todo $\sigma \in A_4$ se tiene que $\sigma^2 \in H$.

(iii) Haga la tabla de multiplicar de A_4.

(iv) Cuente los elementos de la tabla anterior que sean cuadrados y llegue a una contradicción.

EJERCICIO 18. Demuestre que el grupo de Klein es un subgrupo normal de A_4 y que es abeliano.

EJERCICIO 19. [Carmichael [4], Ejercicio 30, página 39]. Sea $G \subseteq S_{16}$ el subgrupo generado por las ocho permutaciones:

$$(1,3)(2,4);\ \ (5,7)(6,8);\ \ (9,11)(10,12);\ \ (13,15)(14,16)$$
$$(1,3)(5,7)(9,11);\ \ (1,2)(3,4)(13,15)$$
$$(5,6)(7,8)(13,14)(15,16);\ \ (9,10)(11,12).$$

(i) Muestre que $[G,G]$ lo generan las cuatro primeras permutaciones listadas arriba.
(ii) Muestre que el orden de $[G,G]$ es 16.
(iii) Por la parte (i) se tiene que $\alpha := (9,11)(10,12)(13,15)(14,16) \in [G,G]$. Muestre que α no es un conmutador.

EJERCICIO 20. Si G es cualquier grupo, dados dos elementos $a, b \in G$, diremos que a es *conjugado* de b si existe otro elemento $g \in G$ tal que $a = gbg^{-1}$. (Esta es la misma definición dada antes de 4.10, para permutaciones). Demuestre que ésta es una relación de equivalencia. Sus clases de equivalencia se conocen como las *clases de conjugación* de G.

EJERCICIO 21. [S. W. Golomb]. Sea G un grupo finito. Demuestre que dos elementos cualesquiera $a, b \in G$ son conjugados si y sólo si se encuentran simétricamente colocados, con respecto a la diagonal principal, en la tabla de multiplicar de G. Recuerde que los elementos de G se pueden escribir como $g = uv$ con u en la columna cero y v en el renglón cero de la tabla de multiplicar de G.

EJERCICIO 22. Usando el ejercicio anterior y la tabla de multiplicar del grupo diédrico D_6 (simetrías del triángulo equilátero), encuentre los elementos conjugados en D_6 y liste sus clases de conjugación.

EJERCICIO 23. [G. T. Hogan]. (Otra demostración de que A_4 no tiene subgrupos de orden 6).

(i) Suponga que H es un subgrupo de A_4 de orden 6. Concluya que H tiene un elemento h de orden 2.
(ii) Observe que H contiene al menos 2 de los elementos de orden 3 de A_4.
(iii) Si t es un elemento de orden 3 en H, concluya que que tht^{-1} debe estar en H y tiene orden 2.

(iv) Observe que si $tht^{-1} = h$, entonces t y h conmutan y th tiene orden 6, lo cual no es posible. Se sigue que $tht^{-1} = k$ es un segundo elemento de orden 2 en H. Observe que hk es un tercer elemento de orden 2 en H. Concluya que $V = \{1, h, k, hk\}$ es un subgrupo de H, lo cual contradice el teorema de Lagrange.

EJERCICIO 24. Sea $H \subseteq G$ un subgrupo. Demuestre que $H \lhd G$ si y sólo si H es una unión de clases de conjugación de G.

Capítulo 6

Homomorfismos e isomorfismos

AHORA QUE YA HEMOS ESTUDIADO varios ejemplos de grupos podríamos pensar en cómo relacionar un grupo con otro, para empezar a pensar en cómo clasificar los grupos, i.e., en cómo distinguirlos si son diferentes o en cómo identificarlos si no son tan diferentes. Con este fin, observemos que los grupos son *conjuntos* junto con una *estructura algebraica* montada en ellos y dada por la operación binaria correspondiente, entonces dados dos grupos G y G', para relacionarlos, pensándolos como conjuntos, podemos considerar funciones entre ellos:

$$\phi : G \to G'$$

y como también debemos tomar en cuenta las operaciones binarias de los dos grupos G y G' es natural que se pida que la función ϕ anterior *respete* ambas operaciones, es decir, que para cualesquiera $a, b \in G$ se tenga que:

$$\phi(a \cdot b) = \phi(a) \cdot \phi(b)$$

donde el producto $a \cdot b$ en la izquierda es el producto de G, y el producto $\phi(a) \cdot \phi(b)$ en la derecha es el producto de G'.

Si una función $\phi : G \to G'$ entre grupos satisface que $\phi(ab) = \phi(a)\phi(b)$, para todos los $a, b \in G$, diremos que ϕ es un *homomorfismo* de G en G'.

Ya que hemos pedido que un homomorfismo $\phi : G \to G'$ respete las operaciones de ambos grupos y ya que estamos en este asunto de ser respetuosos, ¿por qué no le pedimos a ϕ que respete los *neutros* de ambos grupos? o ¿por qué no le pedimos a ϕ que respete la operación de tomar inversos en cada uno de los dos grupos involucrados? Todo esto es natural y viene *gratis* de la definición de homomorfismo:

LEMA 6.1. *Sea $\phi : G \to G'$ un homomorfismo de grupos. Entonces,*

(1) *$\phi(e) = e'$, donde $e \in G$ y $e' \in G'$ son los neutros respectivos.*
(2) *Si $\sigma \in G$, entonces $\phi(\sigma^{-1}) = \phi(\sigma)^{-1}$, donde a la izquierda σ^{-1} es el inverso de σ en G y a la derecha $\phi(\sigma)^{-1}$ es el inverso de $\phi(\sigma)$ en G'.*

Demostración. Para (1), como $ee = e$ en G, entonces

$$\phi(e)\phi(e) = \phi(ee) = \phi(e)$$

en G', de donde cancelando un factor $\phi(e)$ en G' se sigue que $\phi(e) = e'$.

Para (2), como $aa^{-1} = e$ en G, entonces

$$\phi(a)\phi(a^{-1}) = \phi(aa^{-1}) = \phi(e) = e'$$

(donde en la última igualdad usamos la parte (1)). Despejando $\phi(a^{-1})$ de la igualdad anterior se sigue el resultado deseado. □

Ejemplo 1. Si G es cualquier grupo, la *función identidad*

$$\mathrm{id}_G : G \to G$$

dada por $\mathrm{id}_G(\sigma) = \sigma$, es un homomorfismo.

Ejemplo 2. Si G y G' son dos grupos arbitrarios, la función constante $f(\sigma) = e'$ (el neutro de G'), es un homomorfismo $f : G \to G'$.

Ejemplo 3. Si $G = (\mathbb{R}_{>0}, \cdot)$ es el grupo multiplicativo de los números reales positivos, $\mathbb{R}_{>0} = \{x \in \mathbb{R} : x > 0\}$ y si $G' = (\mathbb{R}, +)$ es el grupo aditivo de los números reales, la función *logaritmo natural*

$$\log : \mathbb{R}_{>0} \to \mathbb{R}$$

es un homomorfismo ya que

$$\log(ab) = \log(a) + \log(b)$$

como el lector debe recordar.

Ejemplo 4. Análogamente, la *función exponencial*

$$\exp : \mathbb{R} \to \mathbb{R}_{>0}$$

dada por $\exp(x) = e^x$ (aquí $e = 2.7182\ldots$ es la base de los logaritmos naturales), es un homomorfismo ya que

$$\exp(a + b) = \exp(a)\exp(b)$$

como el lector seguramente recuerda.

Ejemplo 5. Sea $G = \mathrm{GL}(2, \mathbb{R})$ el grupo multiplicativo de las matrices 2×2 con entradas en $\mathbb{R}$ y determinante $\neq 0$. Sea $G' = \mathbb{R}^*$ el grupo multiplicativo de los reales distintos de cero. La *función determinante*

$$\det : \mathrm{GL}(2, \mathbb{R}) \to \mathbb{R}^*$$

es un homomorfismo ya que el determinante de un producto de matrices cuadradas es el producto de los determinantes. El ejemplo se generaliza al grupo $G = \mathrm{GL}(n, \mathbb{R})$ de matrices invertibles $n \times n$ con entradas en $\mathbb{R}$.

Ejemplo 6. Sea $G = S_n$ el grupo simétrico en n letras (con $n \geq 2$) y sea $G' = \{1, -1\}$ el grupo multiplicativo con neutro 1 y tal que $(-1)(-1) = 1$. La *función signo*

$$\operatorname{sgn} : S_n \to \{1, -1\}$$

dada por

$$\operatorname{sgn}(\sigma) := \begin{cases} +1 & \text{si } \sigma \text{ es par} \\ -1 & \text{si } \sigma \text{ es impar} \end{cases}$$

es un homomorfismo, ya que el producto de permutaciones pares es par, el producto de permutaciones impares es impar y el producto de una permutación par por una impar, en cualquier orden, es impar.

Ejemplo 7. Sea $G = (\mathbb{Z}, +)$ el grupo aditivo de los enteros y sea $\mathbb{Z}/n\mathbb{Z}$, para $n \geq 1$ un entero fijo, el grupo aditivo de los énteros módulo n. La función

$$\rho : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$$

dada por $\rho(x) = [x]$ (la clase residual de x módulo n) es un homomorfismo.

Ejemplo 8. El ejemplo anterior se generaliza como sigue: si $N \lhd G$ es un subgrupo normal se tiene una función natural del grupo G en el grupo cociente G/N:

$$\rho : G \to G/N$$

dada por $\rho(\sigma) := \sigma N$ (la clase lateral izquierda de σ). Claramente es una función, ya que a cada elemento de G le corresponde una única clase lateral izquierda en G/N. La función ρ es un homomorfismo ya que si $\sigma, \tau \in G$, entonces

$$\rho(\sigma\tau) = (\sigma\tau)N = \sigma N \tau N = \rho(\sigma)\rho(\tau)$$

(la penúltima igualdad por la definición del producto en G/N). Al homomorfismo $\rho : G \to G/N$ anterior se le llama el *homomorfismo canónico*. Es claro que siempre es *suprayectivo*.

Cuando de respetar se trata, un homomorfismo es bastante respetuoso:[1]

PROPOSICIÓN 6.2. *Sea $\phi : G \to G'$ un homomorfismo de grupos.*

(1) *Si $H \subseteq G$ es un subgrupo, entonces $\phi(H) \subseteq G'$ también es un subgrupo.*
(2) *Si $H \lhd G$, entonces $\phi(H) \lhd G'$.*
(3) *Si $K' \subseteq G'$ es un subgrupo, entonces $\phi^{-1}(K') \subseteq G$ también es un subgrupo.*

[1] Sea $f : A \to B$ cualquier función. Si $M \subseteq A$ es un subconjunto, la *imagen directa* de M es el conjunto

$$f(M) := \{f(x) : x \in M\} \subseteq B.$$

Si $N \subseteq B$ es cualquier subconjunto, la *imagen inversa* de N es el conjunto

$$f^{-1}(N) := \{x \in A : f(x) \in N\} \subseteq A.$$

(4) *Si* $H' \lhd G'$, *entonces* $\phi^{-1}(H) \lhd G'$.

Demostración. Para (1), como $e' = \phi(e)$ por el lema anterior, y como $e \in H$, entonces $e' \in \phi(H)$. Si $a, b \in \phi(H)$, entonces $a = \phi(\alpha)$ y $b = \phi(\beta)$ con $\alpha, \beta \in H$. Se tiene así que $ab = \phi(\alpha)\phi(\beta) = \phi(\alpha\beta)$, con $\alpha\beta \in H$, y por lo tanto $ab = \phi(\alpha\beta) \in \phi(H)$. Si $a \in \phi(H)$, entonces $a = \phi(\alpha)$ con $\alpha \in H$ y por lo tanto $a^{-1} = \phi(\alpha)^{-1} = \phi(\alpha^{-1})$, la última igualdad por el lema anterior. Ahora, como $\alpha \in H$ y H es grupo, entonces $\alpha^{-1} \in H$ y por lo tanto $a^{-1} = \phi(\alpha^{-1}) \in \phi(H)$.

Las partes (2) y (3) las dejamos como un ejercicio. Para (4), queremos mostrar que

$$a\phi^{-1}(K')a^{-1} \subseteq \phi^{-1}(K') \quad \text{para toda } a \in G.$$

Para ésto, sea $\sigma \in \phi^{-1}(K')$ cualquier elemento. Entonces, $\phi(\sigma) \in K'$ y $\phi(a) \in G'$, y como $K' \lhd G'$, entonces

$$\phi(a)\phi(\sigma)\phi(a)^{-1} \in K',$$

es decir, $\phi(a\sigma a^{-1}) \in K'$ y por lo tanto $a\sigma a^{-1} \in \phi^{-1}(K')$, como se quería. □

El núcleo de un homomorfismo. Si $\phi : G \to G'$ es un homomorfismo de grupos, y si consideramos el subgrupo trivial $\{e'\} \lhd G'$, por la proposición anterior su imagen inversa

$$\phi^{-1}\{e'\} \subseteq G$$

es un subgrupo normal de G. Por su importancia se le suele distinguir y se le llama el *núcleo* del homomorfismo ϕ y se denota mediante

$$\ker(\phi) = \phi^{-1}\{e'\} := \{a \in G \,:\, \phi(a) = e'\} \lhd G.$$

Parte de la importancia del núcleo $\ker(\phi) \lhd G$ radica en el resultado siguiente:

PROPOSICIÓN 6.3. *Sea* $\phi : G \to G'$ *un homomorfismo de grupos. Entonces,* ϕ *es inyectivo si y sólo si* $\ker(\phi) = \{e\}$ *es el subgrupo trivial de* G.

Demostración. Si $\phi : G \to G'$ es inyectivo y si $g \in \ker(\phi)$, entonces $\phi(g) = e'$ y como $\phi(e) = e'$ por el lema 6.1, entonces $\phi(g) = \phi(e)$ y la inyectividad de ϕ implica entonces que $g = e$ y por lo tanto $\ker(\phi) = \{e\}$.

Recíprocamente, si $\ker(\phi) = \{e\}$, supongamos que $\phi(a) = \phi(b)$, para $a, b \in G$. Entonces, $\phi(a)\phi(b)^{-1} = e'$, i.e., $\phi(ab^{-1}) = e'$ y por lo tanto $ab^{-1} \in \ker\phi = \{e\}$, i.e., $ab^{-1} = e$ por lo que $a = b$ y así ϕ es inyectiva. □

La imagen de un homomorfismo. Si $\phi : G \to G'$ es un homomorfismo de grupos, y si consideramos el subgrupo total $G \lhd G$, por la proposición 6.2 anterior su imagen directa

$$\phi(G) \subseteq G'$$

es un subgrupo normal de G'. Por su importancia se le suele distinguir y se le llama la *imagen* del homomorfismo ϕ y se denota mediante

$$\text{Im}\,(\phi) = \phi(G) := \{\phi(a) \in G' \,:\, a \in G\} \lhd G'.$$

Así como el núcleo $\ker(\phi)$ detecta cuándo un homomorfismo es inyectivo, la imagen $\text{Im}\,(\phi)$ detecta cuándo un homomorfismo es suprayectivo, sólo que en este caso el resultado es muy sencillo:

Un homomorfismo $\phi : G \to G'$ es suprayectivo si y sólo si $\text{Im}\,(\phi) = G'$, y se sigue directamente de la definición de suprayectividad.

Isomorfismos. Cuando un homomorfismo de grupos $\phi : G \to G'$ es inyectivo y suprayectivo (i.e., cuando es biyectivo), diremos que $\phi : G \to G'$ es un *isomorfismo*. También diremos que G y G' son grupos *isomorfos* cuando exista un isomorfismo entre ellos. A veces usaremos la notación $G \simeq G'$ para denotar el hecho de que G y G' sean isomorfos.

Si $\phi : G \to G'$ es un isomorfismo de grupos, como la función ϕ es biyectiva, tiene una función inversa $\phi^{-1} : G' \to G$ que también es biyectiva. De hecho, es un isomorfismo y para probar ésto sólo falta ver que $\phi^{-1} : G' \to G$ es un homomorfismo de grupos. Para esto, sean $a, b \in G'$. Como ϕ es biyectiva, existen elementos únicos $\alpha, \beta \in G$ tales que $a = \phi(\alpha)$ y $b = \phi(\beta)$. Se tiene entonces que $\phi(\alpha\beta) = \phi(\alpha)\phi(\beta) = ab$ y por lo tanto

$$\phi^{-1}(ab) = \alpha\beta = \phi^{-1}(a)\phi^{-1}(b).$$

Hemos así probado la primera parte del resultado siguiente:

LEMA 6.4. (1) *Si $\phi : G \to G'$ es un isomorfismo de grupos, entonces su inversa $\phi^{-1} : G' \to G$ también es un isomorfismo.*

(2) *Si $\phi : G \to G'$ y $\psi : G' \to G''$ son isomorfismos de grupos, entonces la composición*

$$\psi \circ \phi : G \to G' \to G''$$

también es un isomorfismo.

Demostración. Sólo falta observar que la composición de funciones biyectivas es biyectiva y que la composición de homomorfismos también es un homomorfismo ya que, para $a, b \in G$

$$(\psi \circ \phi)(ab) = \psi(\phi(ab)) = \psi(\phi(a)\phi(b)) = \psi(\phi(a))\psi(\phi(b)) = (\psi \circ \phi)(a)(\psi \circ \phi)(b).$$

□

Observación. Si $\phi : G \to G'$ es un isomorfismo de grupos, entonces ϕ establece una correspondencia biyectiva entre los elementos de G y los de G' y respeta la estructura algebraica de G y G' porque ϕ es homomorfismo; por ejemplo, respeta los

elementos neutros y el tomar inversos de elementos. De esta forma, podemos pensar que un isomorfismo de grupos es como una forma de *renombrar* o *re-etiquetar* los elementos de un grupo; de aquí es donde proviene la etimología: *iso* quiere decir *igual* y *morphé* quiere decir *forma*; por lo tanto *isomorfismo* quiere decir que tienen la *misma forma*. Cuando pensemos en clasificar los grupos, estaremos pensando en tratar de distinguirlos cuando tienen forma diferente, es decir, estaremos interesados en decidir cuándo son o no isomorfos.

Observe ahora que si G es cualquier grupo, como la función identidad $\mathrm{id}_G : G \to G$ es un homomorfismo, entonces $G \simeq G$. También, si $G \simeq G'$ se tiene un isomorfismo $\phi : G \to G'$ y por la parte 1 del lema 6.4 la función inversa $\phi^{-1} : G' \to G$ es un isomorfismo y por lo tanto $G' \simeq G$. Finalmente, si $G \simeq G'$ y $G' \simeq G''$, entonces se tienen isomorfismos $\phi : G \to G'$ y $\psi : G' \to G''$, y por la parte 2 del lema 6.4 la composición $\psi \circ \phi : G \to G''$ es un isomorfismo y así $G \simeq G''$. Hemos así mostrado que la relación de *isomorfismo* es una relación de equivalencia en la familia de todos los grupos.

Ejemplo 9. Por el ejemplo 3 se tiene un homomorfismo de grupos

$$\log : \mathbb{R}_{>0} \to \mathbb{R}$$

y por el ejemplo 4 se tiene un homomorfismo de grupos

$$\exp : \mathbb{R} \to \mathbb{R}_{>0}$$

y es bien conocido (¡debe serlo para el lector!) que estas funciones son inversas una de la otra y por lo tanto son biyectivas. Se sigue los grupos $\mathbb{R}$ y $\mathbb{R}_{>0}$ son isomorfos.

Ejemplo 10. Si $G = \langle \sigma \rangle$ es un grupo cíclico finito de orden n, entonces G es isomorfo al grupo aditivo $\mathbb{Z}/n\mathbb{Z}$ de los enteros módulo n. Un isomorfismo está dado por la función:

$$\phi : \langle \sigma \rangle \longrightarrow \mathbb{Z}/n\mathbb{Z}$$

definida mediante $\phi(\sigma^k) := [k]$ (la clase residual de k módulo n). Recuerde que $\langle \sigma \rangle = \{\sigma^0, \sigma, \sigma^2, \sigma^3, \ldots, \sigma^{n-1}\}$ y que $\mathbb{Z}/n\mathbb{Z} = \{[0], [1], [2], [3], \ldots, [n-1]\}$.

Ejemplo 11. Si $G = \langle \sigma \rangle$ es un grupo cíclico infinito, entonces G es isomorfo al grupo aditivo $\mathbb{Z}$. Un isomorfismo está dado por la función

$$\phi : \langle \sigma \rangle \longrightarrow \mathbb{Z}$$

definida mediante $\phi(\sigma^k) = k$. Note que ésta es una función ya que, como probamos en el Capítulo 3, en un grupo cíclico infinito si $m \neq n$ se tiene que $\sigma^m \neq \sigma^n$. La función ϕ es un *homomorfismo* ya que si $\sigma^k, \sigma^t \in G$, entonces

$$\phi(\sigma^k \cdot \sigma^t) = \phi(\sigma^{k+t}) = k + t = \phi(\sigma^k) + \phi(\sigma^t).$$

Es *inyectiva* ya que si $\phi(\sigma^k) = \phi(\sigma^t)$, entonces $k = t$ y por lo tanto $\sigma^k = \sigma^t$. Es *suprayectiva* ya que si $k \in \mathbb{Z}$, entonces $\sigma^k \in G$ y $\phi(\sigma^k) = k$.

Ejemplo 12. Si $\mu_n = \{z \in \mathbb{C} \ : \ z^n = 1\}$ es el grupo (multiplicativo) de raíces n-ésimas de la unidad, entonces μ_n es un grupo cíclico de orden n generado, por ejemplo, por la raíz $\omega = \exp(2\pi i/n)$, de tal forma que

$$\mu_n = \{1 = \omega^0, \omega, \omega^2, \omega^3, \ldots, \omega^{n-1}\}$$

y así, por el ejemplo 10, μ_n es isomorfo a $\mathbb{Z}/n\mathbb{Z}$. Note que a pesar que los elementos de μ_n y de $\mathbb{Z}/n\mathbb{Z}$ son totalmente diferentes, el isomorfismo anterior los identifica de tal forma que desde el punto de vista algebraico son el mismo grupo.

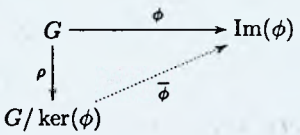
Los ejemplos 10 y 11 nos dicen que cualesquiera dos grupos cíclicos del mismo orden son isomorfos. Si $\langle\sigma\rangle$ es un grupo cíclico finito de orden m, lo denotaremos por $C(m)$.

Dado un homomorfismo de grupos $\phi : G \to G'$, si restringimos su codominio al subgrupo $\text{Im}\,(\phi) \lhd G'$, se tiene un *homomorfismo suprayectivo*

$$\phi : G \to \text{Im}\,(\phi)$$

y el resultado siguiente es de capital importancia en el desarrollo del álgebra:

TEOREMA 6.5 (Primer teorema de isomorfismo de Noether). *Si $\phi : G \to G'$ es un homomorfismo de grupos, entonces ϕ induce un isomorfismo de grupos $\overline{\phi} : G/\ker(\phi) \to \text{Im}(\phi)$, tal que el diagrama siguiente conmuta:*



donde $\rho : G \to G/\ker(\phi)$ es el homomorfismo canónico.

Demostración. Como el homomorfismo canónico $\rho : G \to G/\ker(\phi)$ es suprayectivo, dada cualquier clase lateral izquierda $a\ker(\phi)$ en $G/\ker(\phi)$, para definir $\overline{\phi}(a\ker(\phi)) \in \text{Im}(\phi)$, la primera intención es poner

$$(*) \qquad \overline{\phi}(a\ker(\phi)) = \phi(a);$$

es decir, escogemos como representante $a \in a\ker(\phi)$ y *definimos* $\overline{\phi}$ como ϕ evaluado en el representante elegido. Por supuesto que para que esto tenga sentido tenemos que

mostrar que *no depende* del representante elegido. En efecto, si $ah \in a\ker(\phi)$ es cualquier otro representante, entonces $h \in \ker(\phi)$ y se tiene que

$$\begin{aligned}\phi(ah) &= \phi(a)\phi(h) \quad \text{porque } \phi \text{ es homomorfismo}\\ &= \phi(a)e' \quad \text{porque } h \in \ker(\phi)\\ &= \phi(a)\end{aligned}$$

y por lo tanto el valor de ϕ en cualquier representante de $a\ker(\phi)$ es el mismo. Tiene sentido entonces la definición $(*)$. Note que esta definición de $\overline{\phi}$ hace que el diagrama del teorema conmute, i.e., satisface que

$$\overline{\phi} \circ \rho = \phi.$$

La función $\overline{\phi}$ es un *homomorfismo* ya que si $a\ker\phi$ y $b\ker\phi$ son dos elementos de $G/\ker\phi$, entonces $(a\ker\phi)(b\ker\phi) = ab\ker\phi$ y por lo tanto

$$\begin{aligned}\overline{\phi}((a\ker\phi)(b\ker\phi)) &= \overline{\phi}(ab\ker\phi)\\ &= \phi(ab) \quad \text{por definición de } \overline{\phi}\\ &= \phi(a)\phi(b) \quad \text{porque } \phi \text{ es homomorfismo}\\ &= \overline{\phi}(a\ker\phi)\overline{\phi}(b\ker\phi).\end{aligned}$$

El homomorfismo $\overline{\phi}$ es *inyectivo* ya que si $\overline{\phi}(a\ker\phi) = e'$ (el neutro de $\mathrm{Im}(\phi) \subseteq G'$), entonces $\phi(a) = e'$ por la definición de $\overline{\phi}$. Se tiene así que $a \in \ker\phi$ y por lo tanto $a\ker\phi = \ker\phi$ (el neutro de $G/\ker\phi$), i.e., $\ker\overline{\phi} = \{\ker\phi\}$ y por lo tanto $\overline{\phi}$ es inyectivo.

El homomorfismo $\overline{\phi}$ es *suprayectivo* ya que si $\sigma' \in \mathrm{Im}(\phi)$, entonces como $\phi : G \to \mathrm{Im}(\phi)$ es suprayectivo, existe un $\sigma \in G$ tal que $\phi(\sigma) = \sigma'$ y por lo tanto $\overline{\phi}(\sigma\ker\phi) = \phi(\sigma) = \sigma'$. □

Ejemplo 13. Si $\mathrm{sgn} : S_n \to \{1, -1\}$ es el homomorfismo *signo* (para $n \geq 2$), entonces sgn es suprayectivo y por lo tanto

$$\mathrm{Im}(\mathrm{sgn}) = \{1, -1\}.$$

Por otra parte, el núcleo de sgn es el conjunto de permutaciones $\sigma \in S_n$ tales que $\mathrm{sgn}(\sigma) = 1$, i.e., tales que σ es una permutación *par*. Por lo tanto

$$\ker(\phi) = A_n$$

es el subgrupo alternante de S_n. Note que ésto muestra que $A_n \lhd S_n$.

Ejemplo 14. Sean $G = (\mathbb{R}, +)$ y $G' = (\mathbb{C}^*, \cdot)$ y sea $\phi : \mathbb{R} \to \mathbb{C}^*$ la función dada por $\phi(x) := \cos x + i \operatorname{sen} x$. La función ϕ es un homomorfismo ya que

$$\begin{aligned}\phi(x+y) &= \cos(x+y) + i \operatorname{sen}(x+y)\\ &= \cos x \cos y - \operatorname{sen} x \operatorname{sen} y + i[\operatorname{sen} x \cos y + \operatorname{sen} y \cos x]\\ &= \cos y[\cos x + i \operatorname{sen} x] + i \operatorname{sen} y[\cos x + i \operatorname{sen} x]\\ &= [\cos x + i \operatorname{sen} x][\cos y + i \operatorname{sen} y]\\ &= \phi(x)\phi(y).\end{aligned}$$

La *imagen* de ϕ es el subgrupo de $\mathbb{C}^*$ formado por todos los complejos z tales que $z = \cos x + i \operatorname{sen} x$, i.e., tales que $|z| = 1$. Es decir,

$$\operatorname{Im}(\phi) = \{z \in \mathbb{C} \ : \ |z| = 1\} = S^1 \quad \text{(la circunferencia unitaria en } \mathbb{C}).$$

Ahora, como el neutro del grupo multiplicativo $\mathbb{C}^*$ es el complejo 1, el *núcleo* de ϕ es el subgrupo:

$$\ker(\phi) = \{x \in \mathbb{R} \ : \ \phi(x) = 1\} = \{x \in \mathbb{R} \ : \ \cos x + i \operatorname{sen} x = 1\}$$

y observando que $\cos x + i \operatorname{sen} x = 1$ si y sólo si $x = 2k\pi$ con $k \in \mathbb{Z}$, entonces

$$\ker(\phi) = \{2k\pi \ : \ k \in \mathbb{Z}\} = \langle 2\pi \rangle$$

es el subgrupo cíclico de $\mathbb{R}$ generado por 2π. Por el primer teorema de isomorfismo de Noether se tiene que

$$\mathbb{R}/\langle 2\pi \rangle \simeq S^1.$$

Observe ahora que las clases laterales de $\langle 2\pi \rangle$ en $\mathbb{R}$ tienen un representante $\theta \in \mathbb{R}$ tal que $0 \leq \theta < 2\pi$, i,e, en el intervalo $[0, 2\pi)$ y el isomorfismo anterior *dobla* este intervalo de tal forma que el extremo cerrado 0 encaja en el extremo abierto 2π y forma la circunferencia S^1.

Note que en esta representación geométrica, la suma de ángulos en $\mathbb{R}/\langle 2\pi \rangle$ corresponde al producto de complejos en $S^1 \subseteq \mathbb{C}$ y recordemos que ésto es lo que sucede cuando se multiplican complejos de módulo 1.

El primer teorema de isomorfismo de Noether nos dice que la imagen de cualquier homomorfismo $\phi : G \to G'$ es isomorfa a un grupo cociente: $\operatorname{Im}\phi \simeq G/\ker\phi$. Supongamos ahora que se tiene un grupo cociente G/N, i.e., el subgrupo $N \lhd G$ es normal. Entonces el *morfismo canónico* $\rho : G \to G/N$ es suprayectivo y como $\rho(a) = aN$, el núcleo de ρ es $\ker\rho = N$ y en este caso el primer teorema de Noether es la igualdad $G/N = G/\ker\rho$. Dicho en otras palabras, todo grupo cociente es la imagen de un homomorfismo.

COROLARIO 6.6. *Sea G cualquier grupo.*

(1) *Si ϕ es cualquier homomorfismo con dominio G, entonces $\ker\phi \lhd G$ y la imagen de ϕ es isomorfa al grupo cociente $G/\ker\phi$.*

(2) *Si $N \lhd G$ es cualquier subgrupo normal de G, entonces N es el núcleo del homomorfismo canónico $\rho : G \to G/N$.*

□

Note que en ningún momento hemos dicho que homomorfismos distintos tienen núcleos distintos. Por ejemplo, el homomorfismo identidad $\mathrm{id}_{\mathbb{Z}} : \mathbb{Z} \to \mathbb{Z}$ es diferente del homomorfismo $\phi : \mathbb{Z} \to \mathbb{Z}$ dado por $\phi(m) = -m$ y ambos tienen el mismo núcleo $= \{0\}$.

Supongamos ahora que H y K son dos subgrupos de G con uno de ellos normal, digamos $K \lhd G$. Entonces $H \cap K$ es un subgrupo de G ya que $e \in H$ y $e \in K$ implica que $e \in H \cap K$. Si $a, b \in H \cap K$ entonces $ab \in H$ y $ab \in K$, por lo que $ab \in H \cap K$. Si $a \in H \cap K$, entonces $a^{-1} \in H$ y $a^{-1} \in K$, por lo que $a^{-1} \in H \cap K$. Más aún, $H \cap K$ es subgrupo de H y de K y de hecho, $H \cap K \lhd H$ ya que si $h \in H$ y $a \in H \cap K$, se tiene que $hah^{-1} \in H$ porque $a, h, h^{-1} \in H$, y como $a \in K$, $h \in G$ y $K \lhd G$, entonces $hah^{-1} \in K$. Se sigue que $hah^{-1} \in H \cap K$. Por otra parte, el producto

$$HK = \{hk \ : \ h \in H, k \in K\} \subseteq G$$

es un *subgrupo* de G ya que, $e = ee$ con $e \in H$ y $e \in K$ y así $e \in HK$. Si hk y $h'k'$ son dos elementos de HK, entonces en el producto $(hk)(h'k') = h(kh')k'$, como $K \lhd G$, se tiene que $Kh' = h'K$ y así $kh' = h'\bar{k}$, para algún $\bar{k} \in K$; substituyendo ésto en la igualdad $(hk)(h'k') = h(kh')k'$ se obtiene

$$(hk)(h'k') = h(kh')k' = h(h'\bar{k})k' = (hh')(\bar{k}k') \in HK$$

y por lo tanto HK es cerrado bajo el producto de G. Finalmente, si $hk \in HK$, el inverso

$$(hk)^{-1} = k^{-1}h^{-1} = h^{-1}(hk^{-1}h^{-1}) \in HK$$

ya que $h^{-1} \in H$ y $hk^{-1}h^{-1} \in K$ porque $K \lhd G$. Más aún, $K \lhd HK$ ya que si $k \in K$, entonces $k = ek \in HK$ y por lo tanto K es subgrupo de HK. La normalidad se sigue del hecho de que K es normal en G. Las observaciones anteriores nos dicen que podemos considerar los grupos cociente

$$H/(H \cap K) \quad \text{y} \quad HK/K$$

y el resultado siguiente nos dice que estos dos grupos son isomorfos:

TEOREMA 6.7 (Segundo teorema de isomorfismo de Noether). *Sean H, K subgrupos de G con $K \lhd G$. Entonces, $H \cap K \lhd H$, HK es subgrupo de G, $K \lhd HK$ y se tiene un isomorfismo*

$$H/(H \cap K) \simeq HK/K.$$

Demostración. Sea $\rho : G \to G/K$ el homomorfismo canónico y sea ρ_H su restricción al subgrupo $H \subseteq G$. Es decir, ρ_H es la composición de la inclusión $i : H \hookrightarrow G$ con $\rho : G \to G/K$. Entonces, $\rho_H : H \to G/K$ es un homomorfismo cuyo núcleo es

$$\ker \rho_H = H \cap K,$$

en particular ésto nos da otra demostración de que $H \cap K \lhd H$.

Por otra parte, como por definición $\rho_H(h) = hK$, con $h \in H$, la imagen de ρ_H es el conjunto de clases laterales de K con representantes $h \in H$ y estos representantes se pueden escoger como $hk \in HK$ (con $h \in H, k \in K$), i.e., la imagen de ρ_H es el subgrupo HK/K de G/K.

Por el primer teorema de isomorfismo de Noether se sigue que

$$H/(H \cap K) = H/\ker \rho_H \simeq \operatorname{Im} \rho_H = HK/K.$$

□

Supongamos ahora que los dos subgrupos H y K son normales en G y que además $H \subseteq K \subseteq G$. Entonces, $H \lhd K$ ya que $H \lhd G$. Así, podemos considerar el cociente K/H y éste es un subgrupo de G/H que, más aún, es normal ya que la función

$$\phi : G/H \to G/K$$

dada por $\phi(gH) = gK$, está bien definida, es un homomorfismo y es suprayectiva (lo cual se deja como un ejercicio para el lector) y el núcleo de ϕ es

$$\ker \phi = \{gH \in G/H \ : \ g \in K\} = K/H.$$

Así, $K/H \lhd G/H$ y por lo tanto se puede considerar el cociente $(G/H)/(K/H)$. Ahora, como ϕ es suprayectiva, por el primer teorema de isomorfismo de Noether, se tiene que

$$(G/H)/(K/H) = (G/H)/\ker \phi \simeq \operatorname{Im} \phi = G/K$$

y hemos probado así:

TEOREMA 6.8 (Tercer teorema de isomorfismo de Noether). *Sean H, K dos subgrupos normales de G tales que $H \subseteq K$. Entonces, K/H es un subgrupo normal de G/H y se tiene un isomorfismo*

$$(G/H)/(K/H) \simeq G/K.$$

□

El teorema de Cayley. Si X es cualquier conjunto no vacío, una *permutación* de X es una función biyectiva $\phi : X \to X$. Denotemos con S_X al conjunto de todas las funciones biyectivas de X en X.

TEOREMA 6.9. *El conjunto S_X de todas las permutaciones de un conjunto no vacío X, con la composición de funciones como operación, es un grupo.*

Demostración. Como la composición de funciones biyectivas es biyectiva, S_X es cerrado bajo la composición. La función identidad $\mathrm{id}_X : X \to X$ es biyectiva y funciona como neutra para la composicón de funciones. La composición de funciones es asociativa en general. Finalmente, si $\phi : X \to X$ es biyectiva, entonces tiene inversa $\phi^{-1} : X \to X$ que satisface que $\phi \circ \phi^{-1} = \mathrm{id}_X = \phi^{-1} \circ \phi$. □

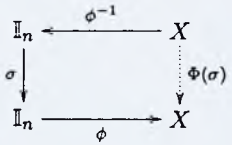
El grupo S_X generaliza la construcción del grupo simétrico S_n, que es el caso particular para $X = \mathbb{I}_n$. Si en lugar de $\mathbb{I}_n$ consideramos cualquier otro conjunto X con n elementos, digamos $X = \{a_1, a_2, \ldots, a_n\}$, podemos considerar el grupo de permutaciones S_X de X,

$$S_X = \{f : X \to X \ : \ f \text{ es biyectiva}\}.$$

Observe ahora que la biyección $\phi : \mathbb{I}_n \to X$ que enumera los elementos de X, i.e., $\phi(k) = a_k$, induce una función

$$\Phi : S_n \to S_X$$

dada como sigue: como ϕ es biyectiva, tiene una inversa $\phi^{-1} : X \to \mathbb{I}_n$ y si $\sigma : \mathbb{I}_n \to \mathbb{I}_n$ es cualquier elemento de S_n, consideremos el diagrama siguiente:



donde la flecha punteada $\Phi(\sigma) : X \to X$ se define mediante la composición

$$\Phi(\sigma) := \phi \circ \sigma \circ \phi^{-1} : X \xrightarrow{\phi^{-1}} \mathbb{I}_n \xrightarrow{\sigma} \mathbb{I}_n \xrightarrow{\phi} X$$

la cual también es biyectiva, porque cada una de las funciones involucradas lo es. Así, $\Phi(\sigma) \in S_X$. La función $\Phi : S_n \to S_X$ es inyectiva porque si $\Phi(\sigma) = \Phi(\tau)$, entonces $\phi \circ \sigma \circ \phi^{-1} = \phi \circ \tau \circ \phi^{-1}$ y, componiendo con ϕ a la derecha se obtiene $\phi \circ \sigma = \phi \circ \tau$ y luego componiendo con ϕ^{-1} a la izquierda, se obtiene que $\sigma = \tau$, como se quería. Como los conjuntos S_n y S_X tienen el mismo cardinal, se sigue que la inyectividad de Φ implica que es *biyectiva*. Finalmente, para mostrar que $\Phi : S_n \to S_X$ es un isomorfismos sólo resta probar que es un homomorfismo. Para esto, si $\sigma, \tau \in S_n$, entonces

$$\begin{aligned}
\Phi(\sigma\tau) &= \phi \circ (\sigma \circ \tau) \circ \phi^{-1} \\
&= \phi \circ (\sigma \circ (\phi^{-1} \circ \phi) \circ \tau) \circ \phi^{-1} \quad \text{insertando id} = \phi^{-1} \circ \phi \text{ entre } \sigma \text{ y } \tau \\
&= (\phi \circ \sigma \circ (\phi^{-1}) \circ (\phi \circ \tau \circ \phi^{-1}) \quad \text{asociando} \\
&= \Phi(\sigma) \circ \Phi(\tau),
\end{aligned}$$

como se requería. Hemos así probado:

PROPOSICIÓN 6.10. *Si X es cualquier conjunto finito con $n \geq 1$ elementos, entonces se tiene un isomorfismo $\Phi : S_n \to S_X$.*

□

Supongamos ahora que se tiene un grupo G, no necesariamente finito. Considerando el conjunto subyacente $X = G$ (olvidando su operación binaria), consideremos el grupo de permutaciones $S_X = S_G$. Mostraremos que G es isomorfo a un subgrupo de S_G, es decir, los elementos del grupo (abstracto) G son (algunas de las) permutaciones (concretas) en S_G. La teoría de grupos tuvo sus inicios estudiando grupos de permutaciones concretos y luego se hizo abstracta, olvidando en apariencia sus orígenes modestos. Sin embargo el resultado que hemos mencionado arriba, debido a Cayley, regresa los grupos abstractos a sus orígenes como grupos de permutaciones. Además de su importancia *filosófica*, en el caso de grupos finitos abstractos, tiene aplicaciones específicas al *representar* estos grupos finitos como grupos de permutaciones finitos también. Antes de proseguir con la demostración de este teorema de Cayley, observemos que aún en el caso de un grupo finito G, al considerar el grupo de permutaciones S_G, como el orden de S_G es el factorial de $|G| = n$, i.e., $|S_G| = n!$, en general el grupo de permutaciones S_G es *muy grande* comparado con el grupo G original. Por eso el teorema de Cayley sólo dice que G es isomorfo a un *subgrupo* de S_G. Para probar el teorema de Cayley, lo primero que debemos hacer es identificar un subgrupo S de S_G que sea un candidato para ser isomorfo a G. Esto es fácil, para cada $g \in G$ definamos la función $\sigma_g : G \to G$ mediante *multiplicación a la izquierda por g*, i.e., $\sigma_g(x) := gx$, para x cualquier elemento de G. Observemos primero que $\sigma_g : G \to G$ es inyectiva, ya que si $\sigma_g(x) = \sigma_g(y)$, entonces $gx = gy$ en G, y multiplicando a la izquierda por g^{-1} se obtiene que $x = y$, como se quería. Segundo, σ_g es suprayectiva, ya que si $z \in G$, sea $x = g^{-1}z \in G$; entonces $\sigma_g(x) = gx = gg^{-1}z = z$. Hemos así mostrado que $\sigma_g : G \to G$ es un función biyectiva, i.e., $\sigma_g \in S_G$. El conjunto de todas estas funciones σ_g es el subconjunto de S_G que necesitamos:

$$S := \{\sigma_g \ : \ g \in G\} \subseteq S_G.$$

A continuación, mostraremos que S es un *subgrupo* de S_G. Para comenzar, observe que para $g = e$ el neutro de G, el elemento $\sigma_e \in S$ correspondiente es el neutro de S_G ya que, para toda $x \in G$, $\sigma_e(x) = ex = x$, i.e., $\sigma_e = \mathrm{id} \in S_G$ es la función identidad, que es el neutro de S_G. Así, $\mathrm{id} = \sigma_e \in S$. Mostraremos ahora que S es *cerrado* bajo la composición de S_G. En efecto, si $\sigma_a, \sigma_b \in S$, entonces

$$(\sigma_a\sigma_b)(x) = \sigma_a(\sigma_b(x)) = \sigma_a(bx) = a(bx) = (ab)x = \sigma_{ab}(x)$$

por lo que

$$\sigma_a\sigma_b = \sigma_{ab} \in S.$$

Finalmente, S es cerrado bajo inversos, ya que si $\sigma_a \in S$, entonces

$$\sigma_{a^{-1}}\sigma_a(x) = \sigma_{a^{-1}a}(x) = \sigma_e(x) = x$$

por lo que $\sigma_a^{-1} = \sigma_{a^{-1}} \in S$.

Resta mostrar que S es isomorfo a G. Para esto primero necesitamos una función

$$\Phi : G \to S \subseteq S_G$$

la cual definimos mediante: $\Phi(a) := \sigma_a$. Observamos ahora que Φ es un homomorfismo ya que si $a, b \in G$, entonces

$$\Phi(ab) = \sigma_{ab} = \sigma_a\sigma_b = \Phi(a)\Phi(b).$$

Segundo, Φ es inyectiva ya que si $\Phi(a) = \Phi(b)$, entonces $\sigma_a = \sigma_b$, en particular, para $x = e$, se tiene que $\sigma_a(e) = \sigma_b(e)$, i.e.,

$$a = ae = \sigma_a(e) = \sigma_b(e) = be = b.$$

Finalmente, Φ es suprayectiva, ya que si $\sigma_a \in S$ entonces obviamente proviene de $a \in G$. Hemos así probado:

TEOREMA 6.11 (Cayley). *Todo grupo es isomorfo a un subgrupo de un grupo de permutaciones.*

□

Ejemplo 15. Para el grupo $G = \mathbb{Z}/3\mathbb{Z} = \{0, 1, 2\}$, cuya tabla de adición es la de los enteros módulo 3:

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

calculemos su representación como grupo de permutaciones usando el teorema de Cayley. Para comenzar, hay tres elementos denotados por $\sigma_0, \sigma_1, \sigma_2$ y definidos, para $x \in \mathbb{Z}/3\mathbb{Z}$, mediante

$$\sigma_0(x) = 0 + x = x, \quad \sigma_1(x) = x + 1, \quad \sigma_2(x) = x + 2,$$

por lo que:

$$\sigma_0 = \begin{pmatrix} 0 & 1 & 2 \\ 0 & 1 & 2 \end{pmatrix}, \quad \sigma_1 = \begin{pmatrix} 0 & 1 & 2 \\ 1 & 2 & 0 \end{pmatrix}, \quad \sigma_2 = \begin{pmatrix} 0 & 1 & 2 \\ 2 & 0 & 1 \end{pmatrix}$$

con tabla de multiplicar dada por:

$\circ$	σ_0	σ_1	σ_2
σ_0	σ_0	σ_1	σ_2
σ_1	σ_1	σ_2	σ_0
σ_2	σ_2	σ_0	σ_1

como el lector puede comprobar fácilmente. Observe ahora que el isomorfismo dado por el teorema de Cayley es *visible* y luce como lo que es: *un cambio de nombres*, $0 \leftrightarrow \sigma_0, 1 \leftrightarrow \sigma_1, 2 \leftrightarrow \sigma_2$; y con las dos operaciones relacionadas mediante: $a+b \leftrightarrow \sigma_a \circ \sigma_b$, por ejemplo $2+2=1 \leftrightarrow \sigma_2 \circ \sigma_2 = \sigma_1$.

Notas. El teorema de Cayley está en [29].

EJERCICIO 1. Muestre que la función $f : (\mathbb{Z}, +) \to (\mathbb{Q}, +)$ dada por $f(n) := n/5$ es un homomorfismo. Calcule su núcleo y su imagen.

EJERCICIO 2. Sea $2\mathbb{Z}$ el grupo aditivo de enteros pares. Defina $g : \mathbb{Z} \to 2\mathbb{Z}$ mediante $g(m) := 2m$. Muestre que g es un isomorfismo.

EJERCICIO 3. ¿Cuáles de las funciones siguientes son homomorfismos?

(i) $f : \mathbb{Q} \to \mathbb{R}_{>0}$ dada por $f(x) := 2^x$.
(ii) $g : \mathbb{R}_{>0} \to \mathbb{R}_{>0}$ dada por $f(x) := 3^{-x}$.
(iii) $h : \mathbb{Q} \to \mathbb{Q}$ dada por $f(x) := 2x + 3$.
(iv) $f : \mathbb{R}^* \to \mathbb{R}^*$ dada por $f(x) := |x|$.

EJERCICIO 4. Encuentre algún criterio en los enteros m, n para que la función

$$f : \mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z} \quad \text{dada por} \quad f[x] := [x]$$

(donde las dos apariciones del símbolo $[x]$ en la definición de f tienen el significado correspondiente al grupo en cuestión) sea un homomorfismo. En el caso cuando f sea un homomorfismo calcule su núcleo.

EJERCICIO 5. Muestre que los grupos aditivos $m\mathbb{Z}$ y $n\mathbb{Z}$ son isomorfos, para cualesquiera $m, n \in \mathbb{Z}$ distintos de cero.

EJERCICIO 6. Sea G cualquier grupo y denotemos con $\mathrm{Aut}(G)$ al conjunto de isomorfismos $f : G \to G$. (Un isomorfismo de un grupo G en sí mismo se llama un *automorfismo*). Demuestre que $\mathrm{Aut}(G)$ es un grupo bajo la composición de homomorfismos.

EJERCICIO 7. Sea G cualquier grupo y para un elemento $\tau \in G$ fijo, definamos la función $c_\tau : G \to G$ mediante $c_\tau(\sigma) := \tau\sigma\tau^{-1}$ (la conjugación de σ por τ). Demuestre

que c_τ es un automorfismo. Los automorfismos c_τ, dados por conjugación por τ, se llaman *automorfismos internos* de G.

EJERCICIO 8. Sea G cualquier grupo y definamos la función $c : G \to \mathrm{Aut}(G)$ como sigue: si $\tau \in G$ sea $c_\tau : G \to G$ el automorfismo interno dado por conjugación por τ. Demuestre que c es un homomorfismo de grupos.

EJERCICIO 9. Construya un homomorfismo inyectivo $\varphi : S_n \to A_{n+2}$. Concluya que la paridad de una permutación no se preserva por los homomorfismos.

EJERCICIO 10. Demuestre que $D_{2n}/R_n \simeq \{1, -1\}$, donde en la derecha se tiene el grupo multiplicativo $\mathbb{Z}^\times$. (Vea el ejercicio 9 del capítulo anterior).

EJERCICIO 11. Demuestre que $\mathrm{GL}(n, \mathbb{R})/\mathrm{SL}(n, \mathbb{R}) \simeq \mathbb{R}^*$. *Sugerencia*: use la función determinante y el primer teorema de isomorfismo de Noether.

EJERCICIO 12. Sea $A = (C_1, \ldots, C_n)$ una matriz $n \times n$, con entradas en $\mathbb{C}$, donde las C_j denotan las columnas de la matriz. Para $\sigma \in S_n$, sea $A^\sigma = (C_{\sigma(1)}, \ldots, C_{\sigma(n)})$ la matriz que se obtiene permutando las columnas de A de acuerdo a σ.

(i) Si I_n es la matriz identidad, demuestre que $\det(I_n^\sigma) = \mathrm{sgn}(\sigma)$.
(ii) Demuestre que $\det(A^\sigma) = \mathrm{sgn}(\sigma)\det(A)$.
(iii) Demuestre que $P_n = \{I_n^\sigma : \sigma \in S_n\}$ es un subgrupo de $\mathrm{GL}(n, \mathbb{C})$.
(iv) Demuestre que la función $\phi : S_n \to P_n$ dada por $\sigma \mapsto I_n^\sigma$ es un isomorfismo de grupos.

Capítulo 7

Productos directos y grupos abelianos finitos

SI G Y K SON DOS GRUPOS, el producto cartesiano

$$G \times K := \{(a, b) \ : \ a \in G, b \in K\}$$

es un grupo con la operación definida componente a componente, i.e., si (a, b), (a', b') están en $G \times K$, se define

$$(a, b) \cdot (a', b') := (aa', bb')$$

donde en la primera componente se tiene el producto de G en la segunda componente al producto de K. El neutro de $G \times K$ es el elemento (e_G, e_K), al que por abuso de notación denotaremos por (e, e), y el inverso de (a, b) es (a^{-1}, b^{-1}). El grupo $G \times K$ se conoce como el *producto directo (externo)* de los grupos G y K.

Ejemplo 1. Si $C(m)$ y $C(n)$ son grupos cíclicos finitos de órdenes m y n respectivamente y si $\text{mcd}(m, n) = 1$, entonces

$$C(m) \times C(n) \simeq C(mn)$$

(el producto directo es isomorfo al grupo cíclico de orden mn). En efecto, si $C(m) = \langle \sigma_m \rangle$, $C(n) = \langle \sigma_n \rangle$ y $C(mn) = \langle \sigma_{mn} \rangle$, la función

$$\phi : C(mn) \to C(m) \times C(n) \quad \text{dada por} \quad \phi(\sigma_{mn}^k) := (\sigma_m^k, \sigma_n^k) = (\sigma_m, \sigma_n)^k$$

es un homomorfismo. Es inyectivo porque si $\phi(\sigma_{mn}^k) = (e, e)$ entonces $\sigma_m^k = e = \sigma_n^k$ por lo que el orden m de σ_m divide a k y el orden n de σ_n divide a k y como $\text{mcd}(m, n) = 1$ entonces $mn | k$ y así $\sigma_{mn}^k = e$. Es suprayectivo porque $C(mn)$ tiene mn elementos que es el orden de $C(m) \times C(n)$. □

Observación. Si $G = H \times K$, entonces G contiene a (una copia de) H y a (una copia de) K como subgrupos normales. En efecto, para H, se tiene la función

$$\phi_H : H \to H \times \{e_K\} \hookrightarrow H \times K$$

dada por $a \mapsto (a, e_K)$ que claramente es un homomorfismo inyectivo. Se sigue que $H \simeq \text{Im}(\phi_H) \subseteq H \times K$. Este subgrupo de $H \times K$ es normal porque si $(h, k) \in H \times K$

y si $(a,e) \in \mathrm{Im}(\phi_H)$ entonces

$$(h,k)(a,e)(h,k)^{-1} = (hah^{-1}, kek^{-1}) = (hah^{-1}, e) \in \mathrm{Im}(\phi_H)$$

porque $hah^{-1} \in H$ ya que h, a, h^{-1} están en H. Similarmente se prueba que $K \simeq \mathrm{Im}(\phi_K) \lhd H \times K$. Finalmente observe que $\mathrm{Im}(\phi_H) \cap \mathrm{Im}(\phi_K) = \{(e,e)\}$.

PROPOSICIÓN 7.1. *Sean G un grupo y H, K subgrupos normales de G tales que $G = HK$ y $H \cap K = \{e\}$. Entonces, $G \simeq H \times K$.*

Demostración. Como $G = HK$ entonces todo elemento $g \in G$ se puede escribir de la forma $g = hk$ con $h \in H$ y $k \in K$. Esta descomposición de g es única porque si $g = h_1k_1$ con $h_1 \in H$ y $k_1 \in K$, entonces $hk = h_1k_1$ por lo que $h^{-1}h_1 = kk_1^{-1}$ y así $h^{-1}h_1 = kk_1^{-1} \in H \cap K = \{e\}$ y consecuentemente $h = h_1$ y $k = k_1$. Podemos entonces definir una función $\phi : G \to H \times K$ mediante $\phi(g) := (h,k)$ si $g = hk$ con $h \in H$ y $k \in K$. La función ϕ es un homomorfismo ya que si $g = hk$ y $g' = h'k'$, entonces $gg' = hkh'k'$ donde observamos que $kh' = h'k$ ya que para cualesquiera $a \in H$ y $b \in K$ se tiene que el conmutador $aba^{-1}b^{-1}$ es tal que $aba^{-1} \in K$ porque $K \lhd G$ y como $b^{-1} \in K$ entonces $aba^{-1}b^{-1} \in K$; similarmente como $a \in H$ y $ba^{-1}b^{-1} \in H$ porque $a^{-1} \in H$ y $H \lhd G$, entonces $aba^{-1}b^{-1} \in H$. Se sigue que $aba^{-1}b^{-1} \in H \cap K = 1$ por lo que $ab = ba$. Así, como $gg' = hkh'k' = hh'kk'$ con $hh' \in H$ y $kk' \in K$ entonces $\phi(gg') = (hh', kk') = (h,k)(h',k') = \phi(g)\phi(g')$.

Claramente ϕ es suprayectiva ya que el par $(h,k) \in H \times K$ proviene del elemento $hk \in G$. Finalmente, ϕ es inyectiva porque si $g = hk$ es tal que $\phi(g) = (h,k) = (e,e)$, entonces $h = e = k$ y así $g = e$. □

Con las hipótesis de la proposición anterior, diremos que G es el *producto directo interno* de H y K.

Hemos así definido dos tipos de productos de grupos. El *producto directo externo* de dos grupos arbitrarios nos sirve para construir nuevos grupos y, como veremos en los capítulos siguientes, el *producto directo interno* nos sirve para describir la estructura interna de un grupo dado. Ambos conceptos se pueden generalizar para definir productos de un número finito de grupos o subgrupos. El más sencillo de generalizar es el producto directo externo: sean $G_1, \ldots, G_s$ grupos arbitrarios; el producto cartesiano

$$G_1 \times \cdots \times G_s := \{(g_1, \ldots, g_s) \ : \ g_i \in G_i\}$$

tiene estructura de grupo con la operación definida componente a componente, con neutro el elemento $(e_1, \ldots, e_s)$, para e_i el neutro de G_i. A este grupo se le llama el *producto directo externo* de los grupos $G_1, \ldots, G_s$. Generalizando lo que sucede en el caso con dos factores (observación después del ejemplo 1), se tienen homomorfismos inyectivos

$$\phi_i : G_i \to G_1 \times \cdots \times G_s$$

definidos por $\phi_i(g) := (e, \ldots, g, \ldots, e)$ (poniendo el elemento $g \in G_i$ en el lugar i y los neutros correspondientes en las otras coordenadas). Si denotamos por $\widetilde{G}_i$ a la imagen de ϕ_i, entonces $\phi_i : G_i \to \widetilde{G}_i$ es un isomorfismo en un subgrupo del producto directo $G_1 \times \cdots \times G_s$.

PROPOSICIÓN 7.2. *Sean $G_1, \ldots, G_s$ grupos arbitarios. Pongamos $G := G_1 \times \cdots \times G_s$. Entonces,*

(1) *Cada $\widetilde{G}_i \lhd G$.*

(2) *$G = \widetilde{G}_1 \cdots \widetilde{G}_s$, i.e., todo elemento $g \in G$ se puede escribir como $g = \bar{g}_1 \cdots \bar{g}_s$ con $\bar{g}_i \in \widetilde{G}_i$.*

(3) *$\widetilde{G}_j \cap \prod_{i \neq j} \widetilde{G}_i = \{e\}$, para cada $j = 1, \ldots, s$. Es decir, la intersección de $\widetilde{G}_j$ con el producto de los otros subgrupos $\widetilde{G}_i$ $(i \neq j)$ es trivial.*

NOTA. Denotamos por $\prod_{i \neq j} \widetilde{G}_i$ al producto $\widetilde{G}_1 \cdots \widetilde{G}_s$ omitiendo al factor $\widetilde{G}_j$.

Demostración. (1): Si $\sigma = (e, \ldots, g, \ldots, e) \in \widetilde{G}_j$ y $h = (h_1, \ldots, h_s) \in G$, entonces

$$\begin{aligned} h\sigma h^{-1} &= (h_1, \ldots, h_s)(e, \ldots, g, \ldots, e)(h_1^{-1}, \ldots, h_s^{-1}) \\ &= (h_1 e h_1^{-1}, \ldots, h_j g h_j^{-1}, \ldots, h_n e h_n^{-1}) \\ &= (e, \ldots, h_j g h_j^{-1}, \ldots, e) \in \widetilde{G}_j \end{aligned}$$

ya que $h_j, g \in \widetilde{G}_j$.

Las partes (2) y (3) son el ejercicio 7. □

Las propiedades de los subgrupos en la proposición anterior nos permiten hacer la definición siguiente: sean $H_1, \ldots, H_s$ subgrupos de G; diremos que G es el *producto directo interno* de los subgrupos $H_1, \ldots, H_s$, si éstos satisfacen las condiciones siguientes:

(1) $H_j \lhd G$.

(2) $G = H_1 \cdots H_s$, i.e., todo elemento g de G se puede escribir (factorizar) como $g = h_1 \cdots h_s$, con los $h_i \in H_i$.

(3) $H_j \cap \prod_{i \neq j} H_i = \{e\}$, para $j = 1, \ldots, s$.

Así, la proposición anterior nos dice entonces que el producto directo externo $G = G_1 \times \cdots \times G_s$ es el producto directo interno $G = \widetilde{G}_1 \cdots \widetilde{G}_s$. El recíproco de esta proposición y que generaliza a 7.1 es:

PROPOSICIÓN 7.3. *Si G es el producto directo interno de los subgrupos $H_1, \ldots, H_s$, entonces*

$$G \simeq H_1 \times \cdots \times H_s.$$

Demostración. La función $\phi : H_1 \times \cdots \times H_s \to G$ dada por $\phi(h_1, \ldots, h_s) := h_1 \cdots h_s$ es suprayectiva por la parte (2) de la definición de producto directo interno. Que es un homomorfismo se prueba como en 7.1 usando las condiciones (1) y (3) de la definición de producto directo interno. Finalmente, es inyectiva porque si $(h_1, \ldots, h_s) \in \ker \phi$, entonces $h_1 \cdots h_s = e$ y así

$$h_j = \prod_{i \neq j} h_i^{-1} \in \prod_{i \neq j} H_i$$

y como $h_j \in H_j$, entonces $h_j \in H_j \cap \prod_{i \neq j} H_i = \{e\}$ por la condición (3), es decir, $h_j = e$ para toda j y por lo tanto $\ker \phi = \{e\}$, como se quería. □

La proposición siguiente da una condición, muy útil, para que un producto de subgrupos normales sea un producto directo:

PROPOSICIÓN 7.4. *Sea G un grupo finito y supongamos que G es el producto de los subgrupos normales $H_1, \ldots, H_s$ y que los órdenes de estos subgrupos son coprimos por pares. Entonces,*

$$G \simeq H_1 \times \cdots \times H_s.$$

Demostración. Sólo falta verificar la condición (3) en la definición de producto directo interno, i.e., que

$$H := H_j \cap \prod_{i \neq j} H_i = \{e\}.$$

Para ésto, observemos que, por Lagrange, $|H|$ es un divisor de cada $|H_j|$ y también de $\ell := |\prod_{i \neq j} H_i|$. Por otra parte, $|\prod_{i \neq j} H_i|$ divide a $\prod_{i \neq j} |H_i|$(vea el ejercicio 9) y así, por transitividad, $|H|$ divide a $\prod_{i \neq j} |H_i|$. Se sigue que $|H|$ divide al máximo común divisor de $|H_j|$ y de $\prod_{i \neq j} |H_i|$, pero éstos son coprimos por la hipótesis, y por lo tanto $H = \{e\}$. □

Grupos abelianos finitos. Aplicaremos los resultados anteriores, sobre productos directos, al caso de grupos abelianos finitos.

TEOREMA 7.5. *Todo grupo abeliano finito G se puede descomponer en un producto directo de grupos cíclicos*

$$G \simeq C(m_1) \times \cdots \times C(m_s),$$

donde cada $C(m_j)$ es un grupo cíclico de orden m_j, y $m_j | m_{j+1}$ para toda $j = 1, \ldots, s-1$.

Demostración. Por inducción sobre $n = |G|$. Si $n = 1$ no hay nada que probar. Supongamos el resultado válido para todos los grupos abelianos de orden menor que $n := |G|$.

Sea $s \geq 1$ el entero tal que G está generado por s elementos pero no está generado por algún conjunto con $s-1$ elementos, y sea $m \geq 1$ el menor entero positivo tal que existe un conjunto $\{g_1, \ldots, g_s\}$ de generadores de G y una relación:

$$mg_1 + a_2g_2 + \cdots + a_sg_s = 0$$

con los $a_j \in \mathbb{Z}$. Nótese que $m > 1$, ya que de lo contrario G estaría generado por los $s-1$ elementos $g_2, \ldots, g_s$.

Poniendo $a_i = mq_i + r_i$ con $0 \leq r_i < m$ para $2 \leq i \leq s$, si tomamos

$$h_1 = g_1 + q_2g_2 + \cdots + q_sg_s,$$

entonces G está generado por $\{h_1, g_2, \ldots, g_s\}$ y además

$$mh_1 + r_2g_2 + \cdots + r_sg_s = mg_1 + a_2g_2 + \cdots + a_sg_s = 0.$$

La minimalidad de m, la igualdad anterior y $0 \leq r_i < m$ implican que $r_2 = \cdots = r_s = 0$ y así $mh_1 = 0$. Mostraremos ahora que

$$G \simeq \langle h_1 \rangle \times \langle g_2, \ldots, g_s \rangle.$$

En efecto, definamos la función $\psi : \langle h_1 \rangle \times \langle g_2, \ldots, g_s \rangle \to G$ mediante $\psi(a,b) := a+b$. Claramente ψ es un homomorfismo de grupos y es suprayectivo ya que $h_1, g_2, \ldots, g_s$ generan G. Es inyectivo ya que si $\psi(a,b) = a + b = 0$, poniendo $a = \alpha_1 h_1$, $b = \alpha_2 g_2 + \cdots + \alpha_s g_s$ con $0 \leq \alpha_1 < m$, se tiene que

$$\alpha_1 h_1 + \alpha_2 g_2 + \cdots + \alpha_s g_s = a + b = 0,$$

y por la minimalidad de m y el hecho de que $0 \leq \alpha_1 < m$, se sigue que $\alpha_1 = 0$ y así $a = \alpha_1 h_1 = 0$, y consecuentemente $b = 0$ también.

Ahora, como el grupo $\langle g_2, \ldots, g_s \rangle$ está generado por $s-1$ elementos pero no por $s-2$ elementos, por hipótesis de inducción se puede descomponer como

$$\langle g_2, \ldots, g_s \rangle \simeq \langle \sigma_{m_2} \rangle \times \cdots \times \langle \sigma_{m_s} \rangle,$$

con los $\langle \sigma_{m_j} \rangle$ cíclicos de orden m_j y $m_j | m_{j+1}$. Se sigue que

$$G \simeq \langle h_1 \rangle \times \langle g_2, \ldots, g_s \rangle \simeq \langle h_1 \rangle \times \langle \sigma_{m_2} \rangle \times \cdots \times \langle \sigma_{m_s} \rangle$$

con $\langle h_1 \rangle$ cíclico de orden m. Denotemos con $\sigma_1 := h_1$ al generador de $\langle h_1 \rangle$.

Por la minimalidad de m se tiene que $m \leq m_2$. Escribamos $m_2 = e_2 m + t_2$ con $0 \leq t_2 < m$ y sea $\sigma_1' := \sigma_1 + e_2\sigma_2$. Entonces, G está generado por $\sigma_1', \sigma_2, \ldots, \sigma_s$, y como

$$\begin{aligned} m\sigma_1' + t_2\sigma_2 &= m\sigma_1 + me_2\sigma_2 + t_2\sigma_2 \\ &= m\sigma_1 + (m_2 - t_2)\sigma_2 + t_2\sigma_2 \\ &= m\sigma_1 + m_2\sigma_2 = 0, \end{aligned}$$

ya que $m\sigma_1 = 0$ y m_2 es el orden de σ_2, entonces $t_2\sigma_2 = 0$ y como $0 \leq t_2 < m$ entonces $t_2 = 0$ y así $m_2 = e_2 m + 0$, i.e., $m | m_2$. □

Ejemplo 2. Denotando a un grupo cíclico de orden m por $C(m)$, considere el grupo:

$$G = C(2^2) \times C(2^3) \times C(2^4) \times C(3) \times C(3^5) \times C(3^7),$$

y note que esta descomposición no satisface la conclusión del teorema, sin embargo reagrupando los factores cíclicos:

$$\begin{aligned} G &\simeq (C(2^2) \times C(3)) \times (C(2^3) \times C(3^5)) \times (C(2^4) \times C(3^7)) \\ &\simeq C(2^2 \cdot 3) \times C(2^3 \cdot 3^5) \times C(2^4 \cdot 3^7), \end{aligned}$$

sí se satisface el teorema.

Una consecuencia inmediata de este teorema es que el recíproco del teorema de Lagrange sí es válido para grupos *abelianos* finitos:

COROLARIO 7.6. *Si G es un grupo abeliano finito y k es un divisor de $|G|$, entonces G contiene un subgrupo de orden k.*

Demostración. Por el teorema anterior $G \simeq C(m_1) \times \cdots \times C(m_s)$ y por el ejercicio 11 $|G| = m_1 \cdots m_s$. Así, si k es un divisor de $|G|$, existen divisores n_i de m_i $(1 \leq i \leq s)$ tales que $k = n_1 \cdots n_s$ y por lo tanto $C(n_1) \times \cdots \times C(n_s)$ es isomorfo a un subgrupo de orden k de G. □

Si G es un grupo finito, el *exponente* de G, denotado $e(G)$, es el mínimo común múltiplo de los órdenes de los elementos de G. Es claro entonces que, para toda $x \in G$, $x^{e(G)} = 1 \in G$, y así $e(G)$ divide al orden de G.

COROLARIO 7.7. *Todo grupo abeliano finito G contiene un elemento de orden $e(G)$.*

Demostración. Usando el teorema 7.5 escribamos

$$G \simeq C(m_1) \times \cdots \times C(m_s),$$

con $m_j | m_{j+1}$. Es claro entonces que para todo $\sigma \in G$ se tiene que $\sigma^{m_s} = 1$, y por lo tanto $e(G) \leq m_s$. Por otro lado, $C(m_s)$ es un subgrupo cíclico de G de orden m_s. Si σ es un generador de este subgrupo, entonces $o(\sigma) = m_s$, y como $o(\sigma) \leq e(G)$, entonces $m_s = o(\sigma) \leq e(G) \leq m_s$, i.e., $o(\sigma) = e(G)$. □

COROLARIO 7.8. *Si G es un grupo abeliano finito tal que $e(G) = |G|$, entonces G es cíclico.*

Demostración. Por el corolario anterior el grupo G tiene un elemento de orden $e(G) = |G|$, y por lo tanto genera a G. □

La factorización del teorema anterior la podemos mejorar eligiendo en forma canónica los factores directos. Esto es el contenido del teorema siguiente, pero antes necesitaremos un resultado preliminar:

LEMA 7.9. *Sean G un grupo abeliano finito y p un primo. Pongamos*

$$G_p := \{g \in G \,:\, g \text{ tiene orden una potencia de } p\}.$$

Entonces, G_p es un subgrupo de G cuyo orden es la mayor potencia de p que divide a $|G|$.

Demostración. Claramente $e \in G_p$ y como G es abeliano, si $x, y \in G_p$ entonces el producto xy también tiene orden una potencia de p y así $xy \in G_p$. Se sigue que G_p es un subgrupo de G. Ahora, si p^T es la mayor potencia de p que divide a $|G|$, por el corolario 7.6 G contiene un subgrupo P de orden p^T. En particular los elementos de P tienen orden una potencia de p y por lo tanto $P \subseteq G_p$. Si sucediera que $P \subsetneq G_p$, entonces para el índice $\ell := [G_p : P] \neq 1$, como $|G_p| = |P|\ell = p^T\ell$, se tendría que $p \nmid \ell$, y de nuevo, 7.6 nos da un subgrupo H de G_p de orden ℓ, y por Lagrange los elementos de H tiene orden que divide a ℓ y además su orden es una potencia de p, lo cual es una contradicción porque $p \nmid \ell$. □

TEOREMA 7.10. *Sea G un grupo abeliano finito de orden n. Si $p_1, \ldots, p_s$ son todos los primos distintos que dividen a n, entonces*

$$G \simeq G_{p_1} \times \cdots \times G_{p_s}.$$

Demostración. Como los $|G_{p_i}|$ son coprimos por pares, por 7.4 el producto $G_{p_1} \cdots G_{p_s}$ es directo. Se sigue que $|G_{p_1} \cdots G_{p_s}| = |G_{p_1}| \cdots |G_{p_s}|$ y por el lema previo cada $|G_{p_i}| = p_i^{T_i}$ (la mayor potencia de p_i que divide a $|G| = n$) y así

$$|G_{p_1} \cdots G_{p_s}| = |G_{p_1}| \cdots |G_{p_s}| = p_1^{T_1} \cdots p_s^{T_s} = n = |G|$$

y por lo tanto $G_{p_1} \cdots G_{p_s} = G$. □

Los subgrupos G_p, que aparecen en la descomposición de G del teorema anterior, se llaman las *componentes p-primarias* de G, pero a diferencia de la factorización del teorema 7.5, estas componentes p-primarias en general no son cíclicas. A los grupos finitos cuyo orden es la potencia de un primo (como los grupos G_p anteriores) se les llama *p-grupos* o *p-primarios* si son abelianos.

Usando el teorema 7.5 podemos descomponer cada componente p-primaria en el teorema 7.10 en producto de subgrupos cíclicos, necesariamente p-grupos, y a continuación mostraremos que esta factorización es *única*, salvo por el orden de los factores. Esto lo haremos probando que el número de factores de un orden p^i está unívocamente determinado por el p-grupo abeliano dado. Podemos entonces suponer que G es un p-grupo abeliano finito. Pongamos entonces, para $i = 0, 1, 2, \ldots$

$$G[p^i] := \{x \in G \,:\, x^{p^i} = 1\}.$$

Entonces, como G es abeliano, $G[p^i]$ es un subgrupo de G y se tiene que $G[p^{i-1}] \subseteq G[p^i]$, para $i \geq 1$.

PROPOSICIÓN 7.11. *Sea G un p-grupo abeliano finito y, usando 7.5, escribamos*

$$(*) \qquad G \simeq C_1 \times \cdots \times C_n$$

(el producto directo de n grupos cíclicos $C_j \neq 1$). *Si* $[G[p^i] : G[p^{i-1}]] = p^{n_i}$, *para* $i \geq 1$, *entonces* $n_i - n_{i+1}$ *es el número de factores de orden* p^i *en la factorización* $(*)$.

Demostración. Como $G = C_1 \times \cdots \times C_n$, entonces $G[p^i] = C_1[p^i] \times \cdots \times C_n[p^i]$. En particular, para $G[p]$, como cada subgrupo cíclico no trivial de $G[p]$ tiene orden p y hay n de estos $|C_k[p]| = p$, entonces, ya que $G[p^0] = 1$, se tiene que

$$p^{n_1} := [G[p] : G[p^0] = |G[p]| = p^n.$$

Se sigue que $n_1 = n$ es el número de factores de orden $\geq p$ en $(*)$. Ahora, como

$$\begin{aligned} G[p^2]/G[p] &= \big(G/G[p]\big)[p] \\ &= \big(C_1 \times \cdots \times C_n/C_1[p] \times \cdots \times C_n[p]\big)[p] \\ &\simeq \big(C_1/C_1[p] \times \cdots \times C_n/C_n[p]\big)[p] \qquad \text{(ejercicio 18)} \\ &= \big(C_1/C_1[p]\big)[p] \times \cdots \times \big(C_n/C_n[p]\big)[p] \\ &= C_1[p^2]/C_1[p] \times \cdots \times C_n[p^2]/C_n[p], \end{aligned}$$

se sigue que n_2 es el número de factores de orden $\geq p^2$ en $(*)$, y consecuentemente $n_1 - n_2$ es el número de factores de orden p. El argumento se sigue por inducción. □

Una consecuencia inmediata del teorema 7.5 y del ejemplo 1 (o del teorema 7.10 y de 7.5) es la primera parte del teorema siguiente y la unicidad es la proposición anterior:

TEOREMA 7.12 (Teorema fundamental de los grupos abelianos finitos). *Todo grupo abeliano finito se puede descomponer en producto directo de grupos cíclicos p-primarios, en forma única, salvo el orden de los factores.* □

Los factores cíclicos que aparecen en la descomposición anterior se llaman los *factores invariantes* del grupo abeliano dado.

Notas. Grupos abelianos finitos fueron estudiados originalmente en teoría de números, por ejemplo por Kronecker [47] y Weber [55], [56], pero de hecho su estudio se remonta a los trabajos de Gauss, particularmente sobre la aritmética de formas cuadráticas. En [47] Kronecker, después de definir lo que esencialmente es un grupo abeliano finito, obtiene varias consecuencias de esta definición, en particular:

> «Si θ es cualquier elemento del conjunto considerado, entonces $\theta^k = 1$ para algún entero positivo k. Si k es el menor tal entero, se dice

que θ *pertenece*[1] a k. Si θ pertenece a k y si $\theta^m = 1$, entonces k divide a m.»

Y también demuestra que:

«Existe un "sistema fundamental" de elementos $\theta_1, \theta_2, \theta_3, \ldots$, tales que la expresión $\theta_1^{h_1}\theta_2^{h_2}\theta_3^{h_3}\cdots$, $(h_i = 1, 2, 3, \ldots, n_i)$ representa, en forma única, cada elemento del conjunto dado. Los enteros $n_1, n_2, n_3, \ldots$ a los cuales pertenecen los $\theta_1, \theta_2, \theta_3, \ldots$, respectivamente, satisfacen que cada uno es divisible por su sucesor y el producto $n_1 n_2 n_3 \cdots$ es la totalidad de los elementos del conjunto dado.»

Lo cual es el teorema 7.5.

EJERCICIO 1. Si $G = H \times K$ y $H_1 \lhd H$, $K_1 \lhd K$, demuestre que $H_1 \times K_1 \lhd G$ y que $G/(H_1 \times H_2) \simeq H/H_1 \times K/K_1$.

EJERCICIO 2. Si $G = H \times K$, demuestre que $G/(H \times 1) \simeq K$.

EJERCICIO 3. Si $H \times K = H \times L$, demuestre que $K \simeq L$.

EJERCICIO 4. Dé un ejemplo de un grupo G y subgrupos H, K de G, tales que $G = H \times K = H \times L$ (producto directo interno), pero que $K \neq L$.

EJERCICIO 5. Si G, G' son grupos, demuestre que $G \times G' \simeq G' \times G$.

EJERCICIO 6. Si G es un grupo, considere el producto directo de G consigo mismo: $G \times G$ y sea $\Delta \subseteq G \times G$ la diagonal, i.e.,

$$\Delta := \{(g, g) \ : \ g \in G\}.$$

(i) Demuestre que Δ es un subgrupo de $G \times G$.
(ii) Demuestre que $\Delta \simeq G$.
(iii) Demuestre que $\Delta \lhd G \times G$ si y sólo si G es abeliano.

EJERCICIO 7. Demuestre las partes (2) y (3) de la proposición 7.2.

EJERCICIO 8. Provea los detalles faltantes en la demostración de que la función ϕ en 7.3 es un homomorfismo.

EJERCICIO 9. Si H y K son subgrupos de un grupo finito G, demuestre que

$$|HK| = \frac{|H||K|}{|H \cap K|}.$$

[1] Una forma anticuada, todavía usada en teoría de números, de decir que θ tiene orden k.

Sugerencia: Un argumento de conteo o vea el ejercicio 14 del capítulo 8.

EJERCICIO 10. Si p es un primo, demuestre que $C(p^2) \not\simeq C(p) \times C(p)$.

EJERCICIO 11. Si G es un grupo abeliano finito y si $G = C(m_1) \times \cdots C(m_s)$ es una descomposición de G como en el teorema 7.5, demuestre que $|G| = m_1 \cdots m_s$.

EJERCICIO 12. Si $G = H \times K$, describa el centro de G en términos de los centros de H y de K. (Vea el ejercicio 7 del capítulo 2).

EJERCICIO 13. Si G es un grupo finito y H, K son subgrupos normales de G tales que $G = HK$ y $|G| = |H||K|$, demuestre que G es el producto directo de H y K.

EJERCICIO 14. Si G es un grupo con subgrupos H, H', K, K' tales que $H \simeq H'$ y $K \simeq K'$, y además $H \cap K = 1 = H' \cap K'$, demuestre que los productos directos HK y $H'K'$ son isomorfos.

EJERCICIO 15. Demuestre que todo grupo de exponente 2 es abeliano.

EJERCICIO 16. Si G es el producto directo interno de los subgrupos $H_1, \ldots, H_s$, demuestre que todo $g \in G$ se descompone en forma *única* como $g = h_1 \cdots h_s$, con los $h_i \in H_i$.

EJERCICIO 17. Si $H_1, \ldots, H_s$ son subgrupos normales de G, demuestre que la función $\psi : G \to G/H_1 \times \cdots \times G/H_s$ dada por $\psi(g) := (gH_1, \ldots, gH_s)$, es un homomorfismo suprayectivo con núcleo

$$\ker \psi = \bigcap_{i=1}^{s} H_i.$$

EJERCICIO 18. Si $G = H_1 \times \cdots \times H_s$, $N \lhd G$, $N_i := N \cap H_i$ y se tiene que $N = N_1 \times \cdots \times N_s$, demuestre que

$$G/N \simeq H_1/N_1 \times \cdots \times H_s/N_s.$$

EJERCICIO 19. Sea G un p-grupo abeliano finito de orden $p^n > 1$ y suponga que para todo $\sigma \in G$ se tiene que $\sigma^p = 1$. Demuestre que G es el producto directo de n grupos cíclicos de orden p.

Capítulo 8

Acciones de grupos y un teorema de Frobenius

En un grupo G su operación binaria es una función $G \times G \to G$ que asigna a cada par (σ, τ) de elementos de G el único elemento $\sigma\tau \in G$. Generalizando lo anterior y recordando la motivación en el capítulo 1, si G es un grupo y Y es un conjunto no vacío, una *acción* de G en Y es una función

$$* : G \times Y \to Y$$

que asigna a cada elemento $\sigma \in G$ y $y \in Y$ un único elemento $\sigma * y \in Y$. Como G es un grupo, es natural pedir que esta acción de G en Y satisfaga las propiedades siguientes:

(1) Si e es el neutro de G, entonces para todo $x \in Y$ se tiene que $e * x = x$.

(2) Si $\sigma, \tau \in G$ y $x \in Y$, entonces $(\sigma\tau) * x = \sigma * (\tau * x)$.

En ocasiones, por abuso de notación, dada una acción $* : G \times Y \to Y$, en lugar de la notación $\sigma * x$ usaremos la notación σx. Con ésto, la propiedad 2 de arriba se escribe $(\sigma\tau)x = \sigma(\tau x)$, donde a la izquierda $\sigma\tau$ es el producto de G y el segundo producto $(\sigma\tau)x$ es la acción de $\sigma\tau$ sobre x. En la derecha los productos son los de la acción de G en Y. Si Y es un conjunto en el cual se tiene una acción de G, diremos que Y es un *G-conjunto*.

Ejemplo 1. Si Y es cualquier conjunto no vacío, sea $G \times Y \to Y$ dada por $\sigma * x = x$. Claramente ésta es una acción de G en Y y decimos que G *actúa trivialmente* en Y.

Ejemplo 2. Si Y es cualquier conjunto no vacío, sea $G = S_Y$ el grupo de permutaciones de Y. Entonces G actúa sobre Y permutando sus elementos, i.e., $G \times Y \to Y$ está dada por $\sigma * x = \sigma(x)$ (la función σ calculada en x).

Ejemplo 3. Sea G cualquier grupo y sea $H \subseteq G$ un subgrupo de G. Entonces H actúa sobre G mediante el producto de G, i.e., $H \times G \to G$ está dada por $h * \sigma = h\sigma$ (*traslación a la izquierda*). En particular, si $H = G$ se tiene que el grupo G actúa sobre sí mismo.

Ejemplo 4. Sea G cualquier grupo y sea $H \subseteq G$ un subgrupo de G. Podríamos preguntarnos si H actúa sobre G mediante *traslaciones derechas*, i.e., si la función

$H \times G \to G$ dada por $h * \sigma = \sigma h$ es una acción. Observemos que el primer axioma es válido: si $h = e$, $e * \sigma = \sigma e = \sigma$. Ahora, si $h, k \in H$ y $\sigma \in G$, queremos que se cumpla la igualdad $(hk) * \sigma = h * (k * \sigma)$, i.e., queremos la igualdad $\sigma hk = \sigma kh$. Si esta igualdad es cierta, en particular para $\sigma = e$ se debe tener que $hk = kh$ para todo $h, k \in H$, es decir, el subgrupo H debe ser *abeliano*. Claramente ésta es una condición suficiente y por lo tanto la traslación derecha es una H-acción sobre G si y sólo si H es abeliano.

Ejemplo 5. Sea G cualquier grupo y sea $H \subseteq G$ un subgrupo de G. La función $H \times G \to G$ dada por $h * \sigma = \sigma h^{-1}$ es una acción de H en G (ésta es una traslación a la derecha por el inverso del elemento h).

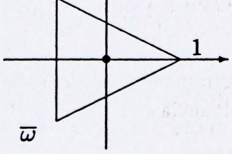
Ejemplo 6. Sea G cualquier grupo y sea $H \lhd G$ un subgrupo normal de G. Entonces, G actúa sobre H mediante conjugación, es decir, mediante la función $G \times H \to H$ dada por $\sigma * h = \sigma h \sigma^{-1}$. La propiedad (1) es obvia y para el axioma (2), sean $\sigma, \tau \in G$ y $h \in H$. Entonces

$$(\sigma\tau) * h = (\sigma\tau)h(\sigma\tau)^{-1} = \sigma(\tau h \tau^{-1})\sigma^{-1} = \sigma(\tau * h)\sigma^{-1} = \sigma * (\tau * h).$$

En particular, G actúa sobre sí mismo por conjugación.

Ejemplo 7. Sea G cualquier grupo y sea $H \lhd G$ un subgrupo normal de G. Entonces G actúa sobre el grupo cociente G/H mediante traslaciones izquierdas, i.e., mediante la función $G \times G/H \to G/H$ dada por $\sigma * (gH) = (\sigma g)H$.

Ejemplo 8. Sea $T = \mu_3 = \{1, \omega, \overline{\omega}\} \subseteq \mathbb{C}$ el grupo de raíces cúbicas de la unidad y veamos a T como los vértices de un triángulo equilátero en $\mathbb{C}$, centrado en el origen y con un vértice en el $1 \in \mathbb{C}$:



Sea G el grupo de simetrías de T. Así, $G = \{e, r, r^2, \rho, \rho r, \rho r^2\}$, donde r es la rotación por un ángulo de 120 grados y ρ es la reflexión con respecto al eje Y. Entonces, G actúa sobre T moviendo sus vértices.

Puntos fijos. Si un grupo G actúa sobre un conjunto Y, interesa saber cómo *mueve* G a los elementos de Y y para ésto suele ser útil estudiar los elementos de Y que *no se*

mueven, i.e., que permanecen fijos bajo la acción de G. Al pensar en elementos que quedan fijos bajo la acción de G, podemos hacerlo desde dos puntos de vista:

(1) Si $\sigma \in G$ está dado, podemos considerar los elementos de Y que permanecen fijos bajo la acción de este σ, y se define

$$Y^{\sigma} := \{x \in Y \ : \ \sigma * x = x\} \subseteq Y.$$

El conjunto Y^{σ} se llama el *conjunto de puntos fijos de* σ.

(2) Si $x \in Y$ es un elemento dado, podemos considerar el subconjunto de elementos del grupo G que dejan fijo a x, y se define

$$G_x := \{\sigma \in G \ : \ \sigma * x = x\} \subseteq G.$$

El conjunto G_x se llama el *subgrupo de isotropía* o *estabilizador* de x, y en efecto es un subgrupo:

LEMA 8.1. *G_x es un subgrupo de G*

Demostración. Claramente $e \in G_x$ ya que $e*x = x$. Si $\sigma, \tau \in G_x$, entonces $(\sigma\tau)*x = \sigma*(\tau*x) = \sigma*x = x$ y por lo tanto $\sigma\tau \in G_x$. Finalmente, si $\sigma \in G_x$, entonces $\sigma^{-1}*x = \sigma^{-1}*(\sigma*x) = (\sigma^{-1}\sigma)*x = e*x = x$ y así $\sigma^{-1} \in G_x$. □

Órbitas. Si Y es un G-conjunto, se define la relación siguiente en Y: $x \sim y$ si existe $\sigma \in G$ tal que $\sigma * x = y$. Cuando $x \sim y$, diremos que x es G-equivalente a y. Ésta es una relación de equivalencia en Y ya que:

(i) Es *reflexiva* ya que $x \sim x$ porque $e * x = x$.

(ii) Es *simétrica* ya que si $x \sim y$ entonces existe $\sigma \in G$ tal que $\sigma x = y$ y así $\sigma^{-1}y = \sigma^{-1}(\sigma x) = ex = x$ y por lo tanto $y \sim x$.

(iii) Es *transitiva* ya que si $x \sim y$ y $y \sim z$, entonces existen $\sigma, \tau \in G$ tales que $\sigma x = y$ y $\tau y = z$. Se sigue que $(\tau\sigma)x = \tau(\sigma x) = \tau y = z$ y así $x \sim z$.

Las clases de equivalencia de la relación anterior se llaman las *órbitas* de la acción de G en Y. A la órbita de $x \in Y$ la denotaremos mediante $[x] = \mathrm{orb}_G(x) = \{\sigma * x \in Y \ : \ \sigma \in G\}$.

Ejemplo 9. Si $\sigma \in S_n$ es una permutación dada y si $G = \langle\sigma\rangle$ es el subgrupo cíclico generado por σ, el grupo G actúa sobre el conjunto $\mathbb{I}_n$ y las órbitas de esta acción son las órbitas de la permutación σ estudiadas previamente. Así, hemos generalizado la definición anterior de órbitas al caso cuando G no necesariamente es cíclico.

Ejemplo 10. Si G actúa trivialmente sobre Y, entonces $\mathrm{orb}_G(x) = \{x\}$, para cada $x \in Y$.

Ejemplo 11. Si $H \subseteq G$ es un subgrupo y H actúa mediante traslaciones izquierdas sobre G, i.e., $H \times G \to H$ está dada por $h * \sigma = h\sigma$, entonces para cada $g \in G$ su órbita es:

$$\begin{aligned} \mathrm{orb}_G(g) &= \{a \in G \,:\, g \sim a\} \\ &= \{a \in G \,:\, a = hg \text{ para algún } h \in H\} \\ &= Hg \quad \text{(la clase lateral derecha de } g\text{)}. \end{aligned}$$

Ejemplo 12. Si G es un grupo y si G actúa sobre sí mismo por conjugación, i.e., $* : G \times G \to G$ está dada por $\sigma * g = \sigma g \sigma^{-1}$, entonces para cada $g \in G$ su grupo de isotropía G_g es:

$$\begin{aligned} G_g &= \{\sigma \in G \,:\, \sigma * g = g\} \\ &= \{\sigma \in G \,:\, \sigma g \sigma^{-1} = g\} \\ &= \{\sigma \in G \,:\, \sigma g = g\sigma\} \\ &= C_G(g) \quad \text{el centralizador de } g \text{ en } G, \end{aligned}$$

(vea el ejercicio 8). Note que las órbitas de esta acción son, para $\sigma \in G$:

$$\mathrm{orb}(\sigma) = \{a \in G \,:\, \sigma \sim a\} = \{a \in G \,:\, a = b\sigma b^{-1} \text{ para algún } b \in G\},$$

es decir, la órbita $\mathrm{orb}(\sigma)$ es la clase de conjugación de σ.

La relación entre órbitas y estabilizadores la da el resultado siguiente, que algunas veces se conoce como el teorema órbita-estabilizador:

TEOREMA 8.2. *Si Y es un G-conjunto, entonces para todo $x \in Y$ se tiene que*

$$|\mathrm{orb}_G(x)| = [G : G_x].$$

Demostración. Definamos $\Phi : \mathrm{orb}_G(x) \to G/G_x$ mediante $\Phi(y) = \sigma G_x$ si $\sigma x = y$. Observe que si $\tau \in G$ es tal que $\tau x = y$ también, entonces $\sigma x = \tau x$ y como

$$\begin{aligned} \sigma x = \tau x &\Leftrightarrow \tau^{-1}\sigma x = x \\ &\Leftrightarrow \tau^{-1}\sigma \in G_x \\ &\Leftrightarrow \sigma G_x = \tau G_x, \end{aligned}$$

entonces Φ está bien definida. La función Φ es *inyectiva* ya que si $\Phi(y) = \Phi(y')$, sean $\sigma, \sigma' \in G$ tales que $\sigma x = y$ y $\sigma' x = y'$ de tal forma que $\Phi(y) = \sigma G_x$ y $\Phi(y') = \sigma' G_x$. Entonces $\sigma G_x = \sigma' G_x$ y por lo tanto $\sigma = \sigma' h$, para algún $h \in G_x$. Se sigue que

$$\begin{aligned} y &= \sigma x = \sigma' h x \\ &= \sigma' x \quad \text{ya que } hx = x \text{ porque } h \in G_x \\ &= y'. \end{aligned}$$

La función Φ es *suprayectiva*, ya que si $\sigma G_x \in G/G_x$, entonces el elemento $y = \sigma x \in \mathrm{orb}_G(x)$ es tal que $\Phi(y) = \sigma G_x$.

Hemos mostrado que Φ es *biyectiva* y por lo tanto

$$|\mathrm{orb}_G(x)| = |G/G_x| = [G : G_x].$$

□

TEOREMA 8.3. *Sea Y un G-conjunto. Si $x, y \in Y$ pertenecen a la misma órbita, entonces G_x y G_y son subgrupos conjugados, en particular son isomorfos.*

Demostración. Como $x \sim y$, entonces existe $\sigma \in G$ tal que $y = \sigma x$. Entonces,

$$\begin{aligned} h \in G_y &\Leftrightarrow hy = y \\ &\Leftrightarrow h(\sigma x) = \sigma x \\ &\Leftrightarrow (\sigma^{-1} h \sigma)x = x \\ &\Leftrightarrow \sigma^{-1} h \sigma \in G_x \\ &\Leftrightarrow \sigma^{-1} h \sigma = h' \in G_x \\ &\Leftrightarrow h = \sigma h' \sigma^{-1} \in \sigma G_x \sigma^{-1}, \end{aligned}$$

y por lo tanto $G_y = \sigma G_x \sigma^{-1}$, como se quería. Finalmente, los grupos conjugados son isomorfos. □

COROLARIO 8.4. *Sea Y un G-conjunto. Si para algún $x \in Y$ se tiene que $G_x \lhd G$, entonces para todos los $y \in \mathrm{orb}_G(x)$ se tiene que $G_y = G_x$.*

Demostración. Por el teorema anterior $G_y = \sigma G_x \sigma^{-1} = G_x$, donde la última igualdad es porque $G_x \lhd G$ por hipótesis. □

TEOREMA 8.5 (Frobenius[1]). *Sean G un grupo finito y Y un G-conjunto finito. Si r es el número de órbitas de Y bajo la acción de G, entonces*

$$r = \frac{1}{|G|} \sum_{\sigma \in G} |Y^\sigma|.$$

Demostración. Mostraremos que $r|G| = \sum_{\sigma \in G} |Y^\sigma|$, y para esto consideremos la tabla dada por el conjunto de pares ordenados

$$T = \{(\sigma, x) \in G \times Y \ : \ \sigma x = x\} \subseteq G \times Y$$

y sea $N = |T|$, el cual es finito ya que G y Y lo son. Contaremos los elementos de la tabla T primero por columnas y luego por renglones. Observemos ahora que, dado un

[1]También conocido como el *lema de Burnside*, pero vea las notas al final del capítulo.

$\sigma \in G$, la columna correspondiente es Y^σ, por la definición de Y^σ, y por lo tanto tiene $|Y^\sigma|$ pares. Como las columnas son disjuntas, se sigue que

$$N = \sum_{\sigma \in G} |Y^\sigma|. \tag{1}$$

Similarmente, dado un $x \in Y$, por definición de G_x hay $|G_x|$ pares de T en el renglón correspondiente a x. Por lo tanto, contando los pares de T por *renglones*, se tiene que

$$N = \sum_{x \in Y} |G_x|. \tag{2}$$

Ahora, por el teorema órbita-estabilizador,

$$|\operatorname{orb}_G(x)| = [G : G_x] = \frac{|G|}{|G_x|} \tag{3}$$

por lo que $|G_x| = |G|/|\operatorname{orb}_G(x)|$. Se sigue que

$$N = \sum_{x \in Y} |G_x| = \sum_{x \in Y} \frac{|G|}{|\operatorname{orb}_G(x)|} = |G| \sum_{x \in Y} \frac{1}{|\operatorname{orb}_G(x)|}. \tag{4}$$

Observamos ahora que $1/|\operatorname{orb}_G(x')|$ es constante para toda $x' \in \operatorname{orb}_G(x)$, de tal forma que si $t := |\operatorname{orb}_G(x)|$, entonces

$$\sum_{x' \in \operatorname{orb}_G(x)} \frac{1}{|\operatorname{orb}_G(x)|} = \overbrace{\frac{1}{t} + \cdots + \frac{1}{t}}^{t \text{ veces}} = 1$$

y así, como r es el número de órbitas de Y, se tiene que

$$\sum_{x \in Y} \frac{1}{|\operatorname{orb}_G(x)|} = r \cdot 1 = r,$$

y substituyendo este valor en (4), queda

$$N = |G| \sum_{x \in Y} \frac{1}{|\operatorname{orb}_G(x)|} = |G| r$$

que substituido en (1) nos da

$$r|G| = \sum_{\sigma \in G} |Y^\sigma|,$$

como se quería. □

Notas. En las primeras dos secciones de la memoria [48], Lagrange rèescribe las demostraciones de Ferrari y Cardano de las fórmulas para resolver por medio de radicales las ecuaciones polinomiales de grados 3 y 4, y en la tercera y cuarta secciones estudia el caso de ecuaciones polinomiales de grado quinto y mayor, considerando permutaciones de las raíces de estas ecuaciones, y en las partes 97 y 98, pp. 370-373 de la

memoria mencionada, demuestra que si $f(x_1, \ldots, x_n)$ es una función racional en n variables (i.e., cociente de dos polinomios en n indeterminadas) y si para cada permutación $\sigma \in S_n$ se define la acción

$$\sigma \cdot f(x_1, \ldots, x_n) := f(x_{\sigma(1)}, \ldots, x_{\sigma(n)}),$$

denotando con $I(f)$ el subgrupo de permutaciones de S_n que dejan fija a f, i.e.,

$$I(f) := \{\sigma \in S_n \ : \ \sigma \cdot f = f\},$$

y si m es el número de funciones racionales distintas de la forma $\sigma \cdot f$, variando σ en S_n, entonces

$$m = \frac{n!}{|I(f)|} = \frac{|S_n|}{|I(f)|}.$$

Éste es el antecedente del *teorema de Lagrange* que demostramos en el capítulo 5, aunque de hecho es más una versión del *teorema órbita-estabilizador* de este capítulo, a partir del cual puede obtenerse otra demostración del teorema de Lagrange (véase el ejercicio 7), ya que el subconjunto $I(f)$ es el estabilizador o subgrupo de isotropía de la función f y m es el número de elementos de la órbita $\text{orb}(f)$ de la acción de S_n en las funciones racionales en n variables. Para más acerca de esta acción del grupo simétrico en el conjunto de funciones racionales en n variables, véase la primera parte del apéndice A.

El teorema de Frobenius en muchas ocasiones es atribuido a Burnside, y ciertamente se encuentra al final de la sección §118 de su libro [2], sin embargo, como observamos previamente, una versión especial ya se encuentra en Lagrange [48] y también en Cauchy [28] (página 386), pero es Frobenius en la parte final de [34], especialmente las páginas 319 y 320, donde enuncia y demuestra el teorema en la versión que vimos y en una nota al pie de página refiere a Cauchy [28], donde se considera el caso *transitivo*. Sin embargo el nombre de Burnside ha quedado unido al teorema, aunque algunas veces también se le conoce como el lema que *no* es de Burnside.

EJERCICIO 1. Sea Y un G-conjunto. Demuestre que la acción de G en Y induce un homomorfismo $\phi : G \to S_Y$. *Sugerencias:* la función ϕ está definida como sigue: si $\sigma \in G$, $\phi(\sigma) \in S_Y$ es la función $\phi(\sigma) : Y \to Y$ dada por $\phi(\sigma)(y) := \sigma * y$. Demuestre que $\phi(\sigma) : Y \to Y$ es biyectiva (y así $\phi(\sigma) \in S_Y$ como se quiere). Demuestre que ϕ es un homomorfismo.

EJERCICIO 2. Recíprocamente, si $\psi : G \to S_Y$ es un homomorfismo, demuestre que ψ induce una acción de G sobre Y mediante $G \times Y \to Y$ dada por $\sigma * x := \phi(\sigma)(x)$.

Los dos ejercicios anteriores nos dicen que dar una G-acción en Y es lo mismo que dar un homomorfismo $\phi : G \to S_Y$.

EJERCICIO 3. Si Y es un G-conjunto con la acción trivial, ver el ejemplo 1, calcule el núcleo del homomorfismo $\phi : G \to S_Y$ correspondiente.

EJERCICIO 4. Si G actúa en sí mismo por conjugación, vea el ejemplo 6, calcule el núcleo del homomorfismo $\phi : G \to S_G$ correspondiente.

EJERCICIO 5. Si Y es un G-conjunto y si $\phi : G \to S_Y$ es el homomorfismo correspondiente, demuestre que

$$\ker \phi = \bigcap_{x \in Y} G_x.$$

EJERCICIO 6. Sea G cualquier grupo y hagamos actuar a G sobre sí mismo por traslaciones izquierdas, vea el ejemplo 3. Demuestre que el homomorfismo $\phi : G \to S_G$ correspondiente es inyectivo.

EJERCICIO 7. Use el teorema de Frobenius para dar otra demostración del teorema de Lagrange.

EJERCICIO 8. Si G es un grupo y $g \in G$, el *centralizador* de g en G, es el conjunto

$$C_G(g) := \{\sigma \in G \ : \ \sigma g = g\sigma\},$$

i.e., es el subconjunto de elementos de G que conmutan con el elemento g dado. Demuestre que $C_G(g)$ es un subgrupo de G, sin usar el ejemplo 12.

EJERCICIO 9. Si G es un grupo y $g \in G$, demuestre que el número de conjugados de g en G es $[G : C_G(g)]$. *Sugerencia:* defina la función $\psi(\sigma g \sigma^{-1}) = \sigma C_G(g)$ entre el conjunto de conjugados de g y las clases laterales izquierdas de $C_G(g)$. Muestre que ψ es biyectiva.

EJERCICIO 10. Si G es un grupo finito y c es el número de clases de equivalencia de la relación de conjugación en G, demuestre que

$$c = \frac{1}{|G|} \sum_{g \in G} |C_G(g)|.$$

EJERCICIO 11. Si X es un conjunto no vacío, por el ejemplo 2 el grupo S_X actúa naturalmente sobre X. Demuestre que sólo hay una órbita de esta acción.

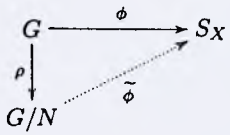
EJERCICIO 12. Si V es un K-espacio vectorial, el grupo aditivo del campo K actúa sobre el grupo abeliano aditivo $(V, +)$ mediante el producto de un escalar por un vector

$$K \times V \to V \quad \text{dada por } (\lambda, v) \mapsto \lambda \cdot v.$$

¿Cuáles son las órbitas de esta acción?

EJERCICIO 13. Si un grupo G actúa sobre un conjunto X, sea $\phi : G \to S_X$ el homomorfismo correspondiente (vea el ejercicio 1) y sea $N = \ker \phi \lhd G$.

(i) Demuestre que si $\rho : G \to G/N$ es el homomorfismo canónico, entonces existe un único homomorfismo $\tilde{\phi} : G/N \to S_X$ tal que el diagrama siguiente es conmutativo:



(ii) Concluya que G/N actúa sobre S_X.

(iii) Demuestre que $\tilde{\phi}$ es inyectivo.

EJERCICIO 14. Si G es un grupo finito y H, K son subgrupos de G, demuestre que

$$|HK| = \frac{|H||K|}{|H \cap K|}.$$

Sugerencias: Sea $Y = G/K$ el conjunto de clases laterales izquierdas de K en G y considere a Y como un H-conjunto mediante traslación izquierda.

(i) Muestre que la órbita de $K \in Y$ es $\mathrm{orb}_H(K) = HK$.

(ii) Concluya de (i) que $|HK|$ es igual a $|K|$ veces el número de clases laterales izquierdas en Y que están en la órbita $\mathrm{orb}_H(K)$.

(iii) Muestre que el estabilizador H_K de $K \in Y$ es $H_K = H \cap K$.

(iv) Use el teorema órbita-estabilizador.

EJERCICIO 15. Si G es un grupo finito y H, K son subgrupos de G, demuestre que para todo $x \in G$ se tiene que

$$|HxK| = \frac{|H||K|}{|H \cap xKx^{-1}|}.$$

Sugerencias:

(i) Muestre que la función $f : HxK \to HxKx^{-1}$ dada por $f(hxk) := hxkx^{-1}$ es biyectiva.

(ii) Observe que xKx^{-1} es un subgrupo de G del mismo orden que K.

(iii) Aplique el ejercicio anterior a los grupos H y xKx^{-1}.

EJERCICIO 16. Si G es un grupo que actúa en el conjunto Y, decimos que la acción es *transitiva* si sólo hay una órbita de la acción. En otras palabras, para cada par de elementos $x, y \in Y$ existe un $\sigma \in G$ tal que $\sigma * x = y$.

El resultado siguiente es un teorema de Jordan: Sea Y un conjunto finito de cardinal $|Y| = n \geq 2$ y supongamos que el grupo finito G actúa transitivamente en Y. Demuestre que existe un elemento $g \in G$ tal que su acción sobre Y no tiene puntos fijos, i.e., tal que $Y^g = \emptyset$. *Sugerencia*: En el teorema de Frobenius, el número de órbitas es 1 y muestre que algún $|Y^g| = 0$.

EJERCICIO 17. Si $G_0 := \{g \in G \ : \ |Y^g| = 0\}$, el ejercicio anterior nos dice que $|G_0| \geq 1$. Esto se puede mejorar. Bajo las condiciones del ejercicio anterior, demuestre que $|G_0| \geq n - 1$. *Sugerencia*: use el teorema órbita-estabilizador para calcular $|G_x|$ y observe que los subgrupos de isotropía tienen al menos al elemento neutro en común y por lo tanto su unión tiene a lo más $n|G_x| - (n-1)$ elementos y así hay, al menos, $n - 1$ elementos de G que no pertenecen a ningún G_x, i.e., que no tienen puntos fijos.

EJERCICIO 18. Si un grupo finito G actúa transitivamente sobre un conjunto finito Y, demuestre que

$$\sum_{\sigma \in G} |Y^\sigma| = |G|.$$

(Lo sobresaliente de esta fórmula es que no incluye al cardinal de Y).

EJERCICIO 19. Después de una función de ópera, cada uno de los asistentes recoge al azar uno de los paraguas que previamente había depositado en el guardaropa. Demuestre que, en promedio, sólo uno de los asistentes recogerá su propio paraguas. (Aquí, *al azar* quiere decir que todas las permutaciones de los paraguas pueden darse). *Sugerencia:* use el ejercicio anterior.

Capítulo 9

Los teoremas de Cauchy y Sylow

SI Y ES UN G-CONJUNTO, con Y y G finitos y si r es el número de órbitas en Y de la acción de G, sean $x_1, \ldots, x_r$ representantes de cada una de las órbitas. Como éstas forman una partición de Y, se tiene que

$$|Y| = \sum_{i=1}^{r} |\operatorname{orb}_G(x_i)|.$$

Note ahora que algunas de las órbitas pueden tener un sólo elemento, y cuando esto sucede este elemento x no lo mueve ningún elemento de G, es decir, queda fijo bajo todo $\sigma \in G$, i.e., $\sigma x = x$ para todo $\sigma \in G$. Pongamos entonces

$$Y^G := \{x \in Y \ : \ \sigma x = x, \ \text{ para todo } \sigma \in G\},$$

es decir, Y^G es la unión de las órbitas con un sólo elemento. Sea $s = |Y^G|$ y observe que $0 \leq s \leq r$. Si $x_1, \ldots, x_s$ son los elementos de las órbitas con un sólo elemento, y $x_{s+1}, \ldots, x_r$ son representantes de las órbitas con más de un elemento, entonces

$$(*) \qquad |Y| = |Y^G| + \sum_{i=s+1}^{r} |\operatorname{orb}_G(x_i)|.$$

Ejemplo 1. Si G es un grupo finito, $Y = G$ y se hace actuar G sobre sí mismo por conjugación (ejemplo 12 del capítulo 8), entonces las órbitas de la acción son las clases de conjugación de G. Observe ahora que las órbitas que tienen un sólo elemento $\operatorname{orb}_G(x) = \{x\}$ satisfacen que $gxg^{-1} = x$, i.e., $gx = xg$ para todo $g \in G$ y por lo tanto x debe estar en el centro $Z(G)$ de G. Se sigue que

$$Y^G = Z(G).$$

Finalmente, si denotamos con $C_1, \ldots, C_t$ las clases de conjugación de G con más de un elemento, la fórmula $(*)$ se vuelve

$$|G| = |Z(G)| + \sum_{i=1}^{t} |C_i|$$

a la que se llama la *ecuación de clases* de G. Ahora, como $|C_i| = |\operatorname{orb}_G(x_i)| = [G : G_{x_i}]$ por el teorema 8.2, la ecuación de clases se puede escribir como

$$|G| = |Z(G)| + \sum_{i=1}^{t} [G : G_{x_i}].$$

TEOREMA 9.1. *Sea G un grupo de orden p^n, para p un entero primo y sea Y un G-conjunto finito. Entonces*

$$|Y| \equiv |Y^G| \ (\text{mód } p).$$

Demostración. Por el teorema 8.2 del capítulo anterior, $|\operatorname{orb}_G(x)| = [G : G_x]$ y por el teorema de Lagrange $[G : G_x]$ divide a $|G| = p^n$, y por lo tanto $p|[G : G_x]$ y así p divide a $|\operatorname{orb}_G(x_i)|$, para $s+1 \leq i \leq r$. Entonces la igualdad $|Y| = |Y^G| + \sum_{i=s+1}^{r} |\operatorname{orb}_G(x_i)|$ de la observación previa implica que p divide a $|Y| - |Y^G|$, como se quería. □

TEOREMA 9.2 (Cauchy). *Si G es un grupo finito y p es un primo que divide a $|G|$, entonces G tiene un elemento de orden p y por lo tanto G tiene un subgrupo de orden p.*

Demostración. Sea Y el conjunto

$$Y = \{(\sigma_1, \ldots, \sigma_p) \ : \ \sigma_j \in G \ \text{ y } \ \sigma_1 \cdots \sigma_p = e\},$$

y observe que $Y \neq \emptyset$ ya que $(e, \ldots, e) \in Y$. Mostraremos que p divide a $|Y|$. En efecto, observando que $(\sigma_1, \ldots, \sigma_p) \in Y \Leftrightarrow \sigma_p = (\sigma_1 \cdots \sigma_{p-1})^{-1}$, se sigue que las primeras $p-1$ componentes de las p-adas de Y pueden ser cualesquiera elementos de G y la última (o la primera) componente está determinada por las otras $p-1$ componentes; por lo tanto $|Y| = |G|^{p-1}$, y como p divide a $|G|$ por hipótesis, entonces p divide a $|Y|$ como se quería.

Consideremos ahora al ciclo $\theta = (1, 2, \ldots, p) \in S_p$ y hagamos actuar θ sobre Y mediante:

$$\theta \cdot (\sigma_1, \ldots, \sigma_p) := (\sigma_{\theta(1)}, \ldots, \sigma_{\theta(p)}) = (\sigma_2, \sigma_3, \ldots, \sigma_p, \sigma_1),$$

donde notamos que $\theta \cdot (\sigma_1, \ldots, \sigma_p) \in Y$, ya que si $(\sigma_1, \ldots, \sigma_p) \in Y$, por definición de Y se tiene que $\sigma_1(\sigma_2 \cdots \sigma_p) = e$, y por lo tanto $\sigma_1 = (\sigma_2 \cdots \sigma_p)^{-1}$ y así $(\sigma_2 \cdots \sigma_p)\sigma_1 = e$, i.e., $(\sigma_2, \ldots, \sigma_p, \sigma_1) \in Y$ como se quería. Se sigue que el grupo cíclico $\langle\theta\rangle$ actúa sobre Y, por iteración de la acción de θ.

Observe ahora que $|\langle\theta\rangle| = p$ y así, por el teorema anterior, se tiene que

$$|Y| \equiv |Y^{\langle\theta\rangle}| \ (\text{mód } p),$$

y como p divide a $|Y|$, la congruencia anterior implica que p divide a $|Y^{\langle\theta\rangle}|$.

Observe también que el ciclo θ (y por lo tanto el grupo $\langle\theta\rangle$) fija a $(\sigma_1, \ldots, \sigma_p)$ si y sólo si $\sigma_1 = \cdots = \sigma_p$. Y por otra parte como $(e, \ldots, e) \in Y^{\langle\theta\rangle}$ por lo que $Y^{\langle\theta\rangle}$ es

no vacío y como p divide a $|Y^{\langle\theta\rangle}|$, se sigue que $Y^{\langle\theta\rangle}$ debe tener al menos p elementos y consecuentemente existe un $(\sigma,\ldots,\sigma) \in Y^{\langle\theta\rangle}$ con $\sigma \neq e$ tal que $\sigma^p = e$, es decir, σ tiene orden p como se quería.

Finalmente, el subgrupo cíclico generado por σ es de orden p ya que σ es de ese orden. □

Ejemplo 2. Note que el teorema de Cauchy no se generaliza para potencias p^k con $k > 1$, i.e., existen grupos finitos G tales que p^k divide a $|G|$ con p primo y $k > 1$, pero que no tienen elementos de orden p^k. Por ejemplo, si $G = C(p) \times C(p)$ es el producto directo de dos copias del grupo cíclico de orden p, entonces $|G| = p^2$, pero es claro que G no tiene elementos de orden p^2.

El normalizador de un subgrupo. Dado un grupo G, denotemos con Y a la familia de todos los subgrupos de G y hagamos actuar G en Y mediante conjugación: si $H \in Y$ y $\sigma \in G$, la acción está dada por

$$\sigma * H := \sigma H \sigma^{-1} \in Y.$$

Claramente $e * H = eHe^{-1} = H$. Y si $\sigma, \tau \in G$, entonces

$$(\sigma\tau) * H = (\sigma\tau)H(\sigma\tau)^{-1} = \sigma(\tau H \tau^{-1})\sigma^{-1} = \sigma(\tau * H)\sigma^{-1} = \sigma * (\tau * H).$$

Ahora, dado un $H \in Y$ consideremos su subgrupo de isotropía

$$G_H := \{\sigma \in G \ : \ \sigma H \sigma^{-1} = H\},$$

y observe que $H \lhd G_H$ ya que claramente H es subgrupo de G_H y es normal porque los elementos σ de G_H son tales que $\sigma H \sigma^{-1} = H$. Más aún, G_H es el mayor subgrupo de G que tiene a H como subgrupo normal, ya que si $K \subseteq G$ es tal que $H \lhd K$ entonces todos los elementos τ de K son tales que $\tau H \tau^{-1} = H$ y por lo tanto $\tau \in G_H$ ya que G_H consiste de todos los elementos de G que fijan a H bajo conjugación. El subgrupo G_H se llama el *normalizador* de H en G y lo denotaremos por $N_G(H)$ ó simplemente $N(H)$ si el grupo G se sobreentiende en el contexto.

LEMA 9.3. *Sea G un grupo finito. Si H es un subgrupo de orden una potencia de un primo p, entonces*

$$[N(H) : H] \equiv [G : H] \ (\text{mód } p).$$

Si H es un grupo finito cuyo orden es una potencia de un primo p, se dice que H es un *p-grupo*.

Demostración. Hagamos actuar G en el conjunto $Y = G/H$ de clases laterales izquierdas de H en G, mediante traslación izquierda, i.e., si $\sigma \in G$ y $\tau H \in G/H$, entonces $\sigma * \tau H = (\sigma\tau)H$. Claramente $Y = G/H$ resulta un G-conjunto y $|G/H| = [G : H]$

por el teorema de Lagrange. Para el subgrupo $H \subseteq G$ denotemos con Y^H al conjunto de puntos fijos de $Y = G/H$ bajo la acción de los elementos de H, i.e.,

$$Y^H = (G/H)^H := \{\tau H \in G/H \ : \ h * (\tau H) = \tau H \ \text{ para todos los } h \in H\}.$$

Observe ahora que

$$h(\tau H) = \tau H \Leftrightarrow \tau^{-1} h \tau H = H \Leftrightarrow \tau^{-1} h \tau \in H$$

y por lo tanto

$$h(\tau H) = \tau H \ \text{ para todos los } h \in H \Leftrightarrow \tau^{-1} h \tau \in H \ \text{ para todos los } h \in H$$

y esto último sucede $\Leftrightarrow \tau \in N(H)$ y consecuentemente,

$$\tau H \in (G/H)^H \Leftrightarrow \tau H \in N(H)/H,$$

es decir la función $Y^H \to N(H)/H$ dada por $\tau H \mapsto \tau H$ es biyectiva y así

$$|(G/H)^H| = |N(H)/H| = [N(H) : H].$$

Finalmente, por 9.1 se tiene que $|G/H| = |Y| \equiv |Y^H| = |(G/H)^H| \pmod{p}$, de donde se sigue que

$$[N(H) : H] = |(G/H)^H| \equiv |G/H| = [G : H] \pmod{p}$$

como se quería. □

COROLARIO 9.4. *Sean G un grupo finito y H un p-subgrupo de G. Si p divide a $[G : H]$ entonces $H \neq N(H)$.*

Demostración. Por el teorema anterior $[N(H) : H] \equiv [G : H] \pmod{p}$ y por hipótesis p divide a $[G : H]$. Se sigue que p divide a $[N(H) : H]$ y por lo tanto $H \neq N(H)$ (ya que $[N(H) : H] \geq 1$). □

Los teoremas de Sylow. Ya hemos llegado al punto en el cual podemos probar los recíprocos parciales del teorema de Lagrange y que constituyen, de alguna forma, el inicio del estudio de los grupos finitos propiamente hablando, es decir, a partir de los teoremas siguientes, debidos a Ludwig Sylow, ya se tiene la herramienta necesaria para comenzar a estudiar los grupos finitos. Nosotros sólo daremos algunas aplicaciones elementales y estudiaremos algunos ejemplos representativos. Recordemos que el teorema de Lagrange nos dice que si G es un grupo finito, el orden de cualquier subgrupo H de G divide al orden de G. El recíproco no es cierto, por ejemplo el grupo alternante A_4, que tiene orden 12, no tiene un subgrupo de orden 6. El primer teorema de Sylow nos dice que si G es finito, entonces G contiene subgrupos de orden ciertos divisores de $|G|$:

TEOREMA 9.5 (Primer teorema de Sylow). *Sea G un grupo finito de orden n y supongamos que p es un primo tal que $n = p^m t$ con $m \geq 1$ y $p \nmid t$. Entonces, G contiene un subgrupo de orden p^j para toda j tal que $1 \leq j \leq m$.*

Demostración. Por inducción sobre j. Si $j = 1$, por el teorema de Cauchy G contiene un subgrupo de orden $p = p^1$. Supongamos ahora que el teorema es válido para $j < m$. Mostraremos que G contiene un subgrupo de orden p^{j+1}. En efecto, sea H un subgrupo de G de orden p^j. Como $j < m$ y $|G| = p^m t$, entonces $m - j \geq 1$ y así p divide a $p^{m-j}t = |G/H| = [G : H]$. El lema anterior implica que p divide a $[N(H) : H] = |N(H)/H|$. Aplicando de nuevo el teorema de Cauchy, se tiene que el grupo cociente $N(H)/H$ tiene un subgrupo K de orden p. Sea $\rho : N(H) \to N(H)/H$ el homomorfismo canónico y sea $L = \rho^{-1}(K) \subseteq N(H)$ la imagen inversa de K. Entonces L es un subgrupo de $N(H)$ que contiene a H (por el teorema de correspondencia entre subgrupos de $N(H)/H$ y subgrupos de $N(H)$ que contienen a H). Observe ahora que $K = \rho(L) = L/H$ y así $|K| = |L/H| = |L|/|H|$ por lo que

$$|L| = |K| \cdot |H| = p \cdot p^j = p^{j+1},$$

como se quería. □

Si G es un grupo finito de orden n y si p es un primo tal que $n = p^m t$ con $m \geq 1$ y $p \nmid t$, a un subgrupo $L \subseteq G$ de orden p^m se le llama un *p-subgrupo de Sylow* de G. En otras palabras, un p-subgrupo de Sylow de G es un p-subgrupo de G de orden máximo.

Observación. Si $L \subseteq G$ es un p-subgrupo de Sylow de G, entonces para todo $\sigma \in G$ el conjugado $\sigma L \sigma^{-1}$ también es un p-subgrupo de Sylow de G. El segundo teorema de Sylow dice que cualesquiera dos p-subgrupos de Sylow de G son conjugados.

TEOREMA 9.6 (Segundo teorema de Sylow). *Sea G un grupo finito de orden n y supongamos que H_1 y H_2 son dos p-subgrupos de Sylow de G. Entonces H_1 y H_2 son conjugados.*

Demostración. La idea es hacer que uno de los dos subgrupos, digamos H_2, actúe sobre las clases laterales izquierdas del otro, digamos sobre $Y = G/H_1$. La acción natural es por traslación izquierda: si $h \in H_2$ y $\sigma H_1 \in Y$, entonces $h(\sigma H_1) = (h\sigma)H_1$. Claramente Y es un H_2-conjunto y por el teorema 9.1 se tiene que

$$|Y^{H_2}| \equiv |Y| \pmod{p},$$

y como H_1 es un p-subgrupo máximo en G, entonces $p \nmid |G/H_1| = |Y|$ por lo que la congruencia anterior implica que $|Y^{H_2}| \neq 0$. Sea pues $\sigma H_1 \in Y^{H_2} = (G/H_1)^{H_2}$. Entonces, $h(\sigma H_1) = \sigma H_1$ para toda $h \in H_2$ y así $\sigma^{-1}h\sigma H_1 = H_1$ para toda $h \in H_2$. Se sigue que $\sigma^{-1}h\sigma \in H_1$ para toda $h \in H_2$, i.e., $\sigma^{-1}H_2\sigma \subseteq H_1$. Finalmente, como $|H_1| = |H_2| = |\sigma^{-1}H_2\sigma|$, la inclusión anterior implica que $\sigma^{-1}H_2\sigma = H_1$, como se quería. □

El tercer teorema de Sylow nos da información sobre el número de p-subgrupos de Sylow de un grupo finito G:

TEOREMA 9.7 (Tercer teorema de Sylow). *Sean G un grupo finito de orden n y p un primo tal que $p|n$. Entonces, el número n_p de p-subgrupos de Sylow de G es congruente con 1 módulo p, y $n_p = [G : N_G(P)]$, donde P es cualquier p-subgrupo de Sylow de G; se sigue que n_p divide al orden n de G.*

Demostración. Sea H un p-subgrupo de Sylow de G y sea Y la familia de todos los p-subgrupos de Sylow de G. Hagamos actuar a H sobre Y mediante conjugación: si $h \in H$ y $L \in Y$, entonces $h * L := hLh^{-1}$. Por el teorema 9.1 se tiene que

$$|Y| \equiv |Y^H| \text{ (mód } p).$$

Ahora, como $Y^H = \{L \in Y \ : \ hLh^{-1} = L \quad \text{para todo } h \in H\}$, entonces $H \subseteq N(L)$ para todo $L \in Y^H$ y además $L \lhd N(L)$. Como H y L son p-subgrupos de Sylow de G, entonces lo son de $N(L)$ y por el segundo teorema de Sylow se sigue que H y L son conjugados en $N(L)$; pero como $L \lhd N(L)$, entonces su único conjugado es él mismo y así $H = L$. Hemos así mostrado que $Y^H = \{H\}$ y por lo tanto, la congruencia $|Y| \equiv |Y^H|$ (mód p) implica que

$$|Y| \equiv 1 \text{ (mód } p),$$

lo cual prueba la primera afirmación del teorema.

Para la segunda afirmación, hagamos actuar G en Y mediante conjugación. Como todos los p-subgrupos de Sylow son conjugados entre sí entonces sólo hay una órbita de esta acción de G en Y, digamos $\text{orb}_G(H)$ para $H \in Y$. Se sigue que

$$(*) \qquad |Y| = |\,\text{orb}_G(H)| = [G : G_H],$$

la última igualdad por el teorema 8.2 del capítulo anterior, donde G_H es el subgrupo de isotropía de H, i.e, $G_H = N_G(H)$ es el normalizador de H en G. Ahora, como $[G : G_H]$ es un divisor de $|G|$ por el teorema de Lagrange, entonces $(*)$ implica que el número de p-subgrupos de Sylow, $|Y|$, divide a $|G|$, como se quería. □

Ejemplo 3. Sea $G = S_3$; entonces $|G| = 3! = 6$. Para el primo $p = 2$, queremos saber cuántos 2-subgrupos de Sylow tiene S_3. Denotemos este número por n_2. Por el tercer teorema de Sylow sabemos que n_2 divide a 6 (y así n_2 puede ser 1, 2, 3, 6) y $n_2 \equiv 1$ (mód 2) (y así n_2 puede ser 1, 3) . Por lo tanto las posibilidades para n_2 son 1 ó 3. Por otra parte, observe que cada una de las transposiciones $(1,2), (1,3), (2,3)$ de S_3 genera un subgrupo cíclico de orden 2 de S_3 y son 2-subgrupos de Sylow de S_3. Así, hay tres 2-subgrupos de Sylow, i.e., $n_2 = 3$.

Para el primo $p = 3$, denotemos con n_3 al número de 3-subgrupos de Sylow de S_3. Entonces las posibilidades para n_3 son: debe dividir a 6, por lo que n_3 puede ser 1, 2, 3, 6; y como $n_3 \equiv 1$ (mód 3), entonces n_3 debe ser 1. El único 3-subgrupo de Sylow de S_3 es $H = \{e, (1,2,3), (1,3,2)\}$.

Ejemplo 4. Sea $G = S_4$. Entonces, $|G| = 4! = 24 = 2^3 \cdot 3$, y recordemos del capítulo 4 la tabla siguiente para el grupo S_4:

Tipo	Número en cada tipo	Orden del elemento	Paridad
(•)	1	1	Par
(• •)	6	2	Impar
(• • •)	8	3	Par
(• • • •)	6	4	Impar
(• •)(• •)	3	2	Par

Para el primo $p = 3$, se tiene que n_3 divide a 24 por lo que puede ser 1, 2, 3, 4, 6, 8, 12, 24. Y como $n_3 \equiv 1 \pmod 3$, las posibilidades para n_3 se reducen a: 1 y 4. Para decidir cuál de estas posibilidades es la correcta, observemos que los 3-subgrupos de Sylow de S_4 son de orden 3 y por lo tanto son cíclicos generados por un elemento de orden 3. Entre los elementos de S_4 los de orden 3 son los 3-ciclos: (1,2,3), (1,2,4), (1,3,4) y (2,3,4). Por lo tanto hay cuatro 3-subgrupos de Sylow, los generados por los ciclos anteriores.

Para el primo $p = 2$, se tiene que n_2 divide a 24 y como $n_2 \equiv 1 \pmod 2$, las posibilidades para n_2 se reducen a: 1 y 3. Para decidir cuál de estas posibilidades es la correcta, observemos que los 2-subgrupos de Sylow de S_4 son de orden 8 y ahora observe que el subconjunto de S_4:

$$K := \{1,\ (1\ 2)(3\ 4),\ (1\ 3)(2\ 4),\ (1\ 4)(2\ 3)\}$$

es un subgrupo normal de S_4 ya que sus elementos son todas aquellas permutaciones de S_4 que tienen la estructura cíclica (•) ó (• •)(• •). Ahora, como $|K| = 4$, entonces K es un 2-subgrupo de S_4 por lo que está contenido en algún 2-subgrupo de Sylow de S_4. También, como los 2-subgrupos de Sylow son conjugados y como K es normal, entonces K está contenido en *todos* los 2-subgrupos de Sylow de S_4. Observe ahora que para cada $\sigma \in S_4$ del tipo (• • • •), el grupo cíclico $\langle\sigma\rangle$ tiene orden 4 y así está contenido en algún 2-subgrupo de Sylow de S_4, y como $\sigma \notin K$, entonces el 2-subgrupo generado por σ y K: $H_\sigma := \langle\sigma, K\rangle$ tiene orden 8 y por lo tanto es un 2-subgrupo de Sylow de S_4. Ahora, viendo la tabla de S_4, observe que hay 6 posibilidades para σ, pero note que

$$\langle\sigma\rangle = \langle\sigma^3\rangle$$

para cualquier σ del tipo (• • • •). Se sigue que $H_\sigma = H_{\sigma^3}$ y así las 6 posibilidades para σ se vuelven a lo más $\frac{6}{2} = 3$ y finalmente se verifica que

$$\langle(1234), K\rangle,\ \langle(1243), K\rangle,\ \langle(1423), K\rangle,$$

son distintos y por lo tanto $n_3 = 3$.

Ejemplo 5. Si $G = S_p$, con p un primo, entonces $|S_p| = p \cdot (p-1)!$ y $p \nmid (p-1)!$ por lo que S_p contiene p-subgrupos de Sylow de orden exactamente p; se sigue que estos p-subgrupos de Sylow deben ser cíclicos generados por un elemento de orden p. Ahora, en S_p hay exactamente

$$\frac{p!}{p \cdot (p-p)!} = (p-1)!$$

p-ciclos. Sea n_p el número de p-subgrupos de Sylow de S_p. Entonces, en cada p-subgrupo de Sylow H de S_p hay $(p-1)$ ciclos de período p, por lo que

$$n_p(p-1) = (p-1)!$$

y así $n_p = (p-2)!$ Note que como $n_p \equiv 1 \pmod{p}$, entonces $(p-2)! \equiv 1 \pmod{p}$ (el teorema de Wilson).

p-grupos. Si p es un primo, un grupo G se dice que es un *p-grupo* si todo elemento de G tiene orden una potencia de p. En el caso cuando G es finito, esta definición coincide con la dada antes de la demostración del lema 9.3:

PROPOSICIÓN 9.8. *Un grupo finito G es un p-grupo si y sólo si el orden de G es una potencia de p.*

Demostración. Si $|G| = p^n$, entonces para todo $g \in G$ como el orden de g divide a $|G| = p^n$, entonces el orden de g es una potencia de p. Recíprocamente, supongamos que existe un primo $q \neq p$ tal que q divida a $|G|$. Entonces, por el teorema de Cauchy existe un $g \in G$ de orden q, en contradicción con la hipótesis de que el orden de todos los elementos de G es una potencia de p. □

El lema siguiente, que es el ejercicio 3 del capítulo 5, nos será útil:

LEMA 9.9. *Sea G cualquier grupo. Si $G/Z(G)$ es cíclico, entonces G es abeliano.*

Demostración. Si $G/Z(G) = \langle \overline{g} \rangle$, con $\overline{g} = gZ(G)$, entonces para cualesquiera $\sigma, \tau \in G$, considerando sus clases laterales $\overline{\sigma}, \overline{\tau} \in G/Z(G)$, las podemos escribir como $\overline{\sigma} = \overline{g^k}$ y $\overline{\tau} = \overline{g^t}$, y así $\sigma = g^k z$ y $\tau = g^t \zeta$, con $z, \zeta \in Z(G)$. Entonces,

$$\sigma\tau = g^k z g^t \zeta = g^k g^t z\zeta = g^t g^k \zeta z = g^t \zeta g^k z = \tau\sigma$$

(donde usamos que z y ζ conmutan con todos los elementos de G y obviamente $g^k g^t = g^t g^k$). □

Regresando a p-grupos:

LEMA 9.10. *Si $G \neq 1$ es un grupo finito de orden p^n con p un primo, entonces el centro de G no es trivial, i.e., $Z(G) \neq 1$.*

Demostración. Haciendo actuar G sobre $Y = G$ por conjugación, por el ejemplo 1, $Y^G = Z(G)$ es el centro de G, y por el teorema 9.1

$$|Z(G)| \equiv |G| \equiv 0 \pmod{p}$$

(la última congruencia porque G es un p-grupo). Se sigue que p divide al orden de $Z(G)$ y así $Z(G) \neq 1$. □

Grupos simples. Un grupo $G \neq 1$ se dice que es *simple* si no tiene subgrupos normales propios. Ejemplos inmediatos están dados por los grupos cíclicos finitos de orden primo: son simples por el teorema de Lagrange.

COROLARIO 9.11. *Si G es un p-grupo finito no abeliano, entonces G no es simple.*

Demostración. Como G no es abeliano, entonces $Z(G) \subsetneq G$ y por el lema $Z(G) \neq 1$, por lo que $1 \neq Z(G) \lhd G$. □

COROLARIO 9.12. *Si p es un primo, todo grupo G de orden p^2 es abeliano.*

Demostración. Si G fuera no abeliano, entonces $Z(G) \neq G$ y como por el lema anterior $Z(G) \neq 1$, entonces $|Z(G)| = p$. Se sigue que $G/Z(G)$ tiene orden p y por lo tanto es cíclico. El resultado se sigue del lema 9.9. □

COROLARIO 9.13. *Todo grupo de orden p^2 es isomorfo a $C(p^2)$ ó a $C(p) \times C(p)$.*

Demostración. Se sigue del corolario anterior y del teorema 7.2. □

Observación. El corolario 9.12 no es válido para grupos de orden p^k con $k \geq 3$, por ejemplo existen grupos de orden p^3 no abelianos, un ejemplo, para $p = 2$, es el grupo de simetrías del cuadrado, i.e., el grupo diédrico D_8 de orden 8.

Grupos de orden pq. A continuación clasificaremos todos los grupos de orden el producto de dos primos distintos. Necesitaremos los resultados siguientes: en el ejercicio 2 del capítulo 5 se pedía probar que si H es un subgrupo de G de índice 2, entonces $H \lhd G$. La proposición siguiente generaliza este ejercicio y para probarla necesitaremos el lema:

LEMA 9.14. *Sea G un grupo arbitario y sea H un subgrupo de índice n en G. Entonces, existe un subgrupo normal N de G que está contenido en H y tal que el índice $[G : N]$ es finito y divide a $n!$.*

Demostración. Sea $Y = \{g_1H, \ldots, g_nH\}$ un sistema completo de representantes de las clases laterales izquierdas de H en G y hagamos actuar G en Y mediante traslaciones, i.e., $g(g_iH) := (gg_i)H$. La acción anterior induce el homomorfismo

$\phi : G \to S_Y$ mediante $\phi(g)(g_iH) := gg_iH$, (vea el ejercicio 1 del capítulo 8). Pongamos $N = \ker \phi \lhd G$. Por el ejercicio 5 del capítulo 8,

$$N = \ker \phi = \bigcap_{g_iH \in Y} G_{g_iH}$$

y como

$$\begin{aligned} G_{g_iH} &= \{g \in G \ : g(g_iH) = g_iH\} = \{g \in G \ : \ gg_i = g_ih \ \text{ para algún } h \in H\} \\ &= \{g \in G \ : \ g \in g_iHg_i^{-1}\} = g_iHg_i^{-1}, \end{aligned}$$

entonces $G_{g_iH} = g_iHg_i^{-1}$, por lo que

$$N = \bigcap_{g_iH \in Y} G_{g_iH} = \bigcap_{g_iH \in Y} g_iHg_i^{-1}$$

de donde se sigue que $N \subseteq H$ ya que una de las clases laterales g_iH es H. Finalmente, por el primer teorema de isomorfismo de Noether, $G/\ker \phi \simeq \text{Im } \phi$ y así

$$[G : N] = [G : \ker \phi] = |\text{Im } \phi|$$

y como Im ϕ es subgrupo de S_n y este grupo tiene orden $n!$, entonces $|\text{Im } \phi|$ divide a $n!$, como se quería. □

PROPOSICIÓN 9.15. *Sea G un grupo finito de orden n y sea p el menor primo que divide a n. Entonces, todo subgrupo de índice p en G es normal.*

Demostración. Sea $H \subseteq G$ un subgrupo de índice $[G : H] = p$. Por el lema anterior existe un subgrupo normal $N \lhd G$, con $N \subseteq H$ y tal que $[G : N]$ divide a $p!$. Mostraremos que $N = H$. Para ésto observamos primero que como $N \subseteq H$ y son finitos, entonces basta mostrar que $|N| = |H|$, ó lo que es lo mismo, que $[G : N] = [G : H]$. Para probar esto último observemos que como $N \subseteq H$, entonces $p = [G : H] \leq [G : N]$ y así $[G : N] \neq 1$. Sea q un primo que divide a $[G : N]$. Como $[G : N]$ divide a $p!$, entonces $q|p!$ y por lo tanto $q \leq p$. Ahora, por el teorema de Lagrange, q también divide a $|G| = n$, y por la minimalidad de p se sigue que $p \leq q$ y por lo tanto $p = q$. Se sigue que $[G : N] = p^r$, y como $p^r = [G : N]$ divide a $p!$, entonces $r = 1$ y consecuentemente $[G : N] = p$, como se quería. □

COROLARIO 9.16. *Si G es un grupo de orden pq, con $p > q$ primos, entonces G no es simple.*

Demostración. Por el teorema de Cauchy G tiene un subgrupo H de orden p y por lo tanto su índice $[G : H] = q < p$; por la proposición anterior $H \lhd G$. □

PROPOSICIÓN 9.17. *Sea G un grupo de orden pq, con $p > q$ primos. Si $p \not\equiv 1$ (mód q), entonces G es cíclico.*

Demostración. Por el teorema de Cauchy G tiene un subgrupo H de orden p y por lo tanto $[G : H] = q$, y como q es el menor primo que divide a $|G|$, por la proposición anterior $H \lhd G$. Hagamos actuar a G sobre H mediante conjugación. Si $h \in H$ observe que

$$(*) \qquad \mathrm{orb}_G(h) = \{h\} \Leftrightarrow \text{para todo } g \in G,\ ghg^{-1} = h \Leftrightarrow h \in H \cap Z(G).$$

Mostraremos que $H \cap Z(G) = H$. Asumiendo ésto por el momento, se sigue que $H \subseteq Z(G)$ y por lo tanto $|Z(G)| = p$ ó $|Z(G)| = pq$. Así, $[G : Z(G)] = q$ ó 1, y por lo tanto $G/Z(G)$ es cíclico. El lema 9.9 implica entonces que G es abeliano y como su orden es el producto de primos distintos, entonces G es cíclico, como se quería.

Resta sólo mostrar que $H \cap Z(G) = H$ y como el orden de H es p, primo, y $H \cap Z(G) \subseteq H$, entonces basta probar que $H \cap Z(G) \neq 1$. Supongamos que $H \cap Z(G) = 1$. Como $|H| = p$, entonces existe un $h \in H$ con $h \neq 1$, y para la órbita $\mathrm{orb}_G(h) \subseteq H$ si se tuviera la igualdad $\mathrm{orb}_G(h) = H$, entonces todo $\tau \in H$ sería conjugado de h por algún elemento de G, en particular para el $1 \in H$ se tendría que $1 = \sigma h \sigma^{-1}$ y así $\sigma = \sigma h$ por lo que, cancelando a σ se tendría que $1 = h$, en contradicción con la hipótesis de que $h \neq 1$. Se sigue que $\mathrm{orb}_G(h) \subsetneq H$ y así

$$|\mathrm{orb}_G(h)| \text{ divide a } |G| = pq \text{ y además } |\mathrm{orb}_G(h)| < |H| = p$$

y por lo tanto $|\mathrm{orb}_G(h)| = q$ porque no puede tenerse que $|\mathrm{orb}_G(h)| = 1$ ya que si esto pasara, por $(*)$ se tendría que $h \in H \cap Z(G)$ con $h \neq 1$, en contradicción con la hipótesis de que $H \cap Z(G) = 1$. Así, $|\mathrm{orb}_G(h)| = q$ para todos los $h \neq 1$ en H, y como $\mathrm{orb}_G(1) = \{1\}$ y las órbitas forman una partición de H, entonces

$$p = |H| = \sum_{h \in H} |\mathrm{orb}_G(h)| = 1 + \sum_{h \neq 1 \text{ en } H} |\mathrm{orb}_G(h)| = 1 + \sum_{h \neq 1} q = 1 + rq$$

por lo que $p \equiv 1 \pmod{q}$, en contradicción con la hipótesis de la proposición. Se sigue que $H \cap Z(G) = H$ como se quería. □

TEOREMA 9.18. *Sea G un grupo de orden pq, con $p > q$ primos.*

(1) *Si G es abeliano, entonces $G = C(pq)$ es cíclico de orden pq.*

(2) *Si G no es abeliano, entonces $p \equiv 1 \pmod{q}$ y $G \simeq \langle a, b \mid a^q = 1 = b^p,\ aba^{-1} = b^r \rangle$, donde r es un entero tal que $1 < r < p$ y $r^q \equiv 1 \pmod{p}$.*

Demostración. (1): Si G es abeliano, como $|G| = pq$ y $\mathrm{mcd}(p, q) = 1$, entonces $G \simeq C(p) \times C(q) \simeq C(pq)$.

(2): Si G no es abeliano, por la proposición anterior $p \equiv 1 \pmod{q}$. Por el teorema de Cauchy G tienen elementos b de orden p y a de orden q. El subgrupo de G generado por a y b tiene elementos de órdenes p y q y por lo tanto debe ser igual a G, i.e., $\langle a, b \rangle = G$. Sean $H = \langle b \rangle$ y $K = \langle a \rangle$. Como $|H| = p$, entonces $[G : H] = q$ y así por 9.15, $H \lhd G$. Se sigue que $aba^{-1} \in H = \langle b \rangle$ y así existe un entero r, $0 \leq r < p$,

tal que $aba^{-1} = b^r$. Si se tuviera que $r = 0$, entonces $aba^{-1} = 1$ y así $ab = a$ por lo que $b = 1$, en contradicción con el hecho de que b es de orden p. Si sucediera que $r = 1$, entonces $aba^{-1} = b$ y así $ab = ba$ y por lo tanto el grupo $\langle a, b\rangle = G$ sería abeliano, en contradicción con la hipótesis de (2). Se sigue que $1 < r < p$. Finalmente, por inducción sobre $j \geq 0$ se prueba que

$$(*) \qquad a^j b a^{-j} = b^{r^j}.$$

En efecto, si $j = 0$ ó 1, el resultado ya se tiene. Supongamos que $(*)$ es verdadera para j. Entonces,

$$a^{j+1} b a^{-(j+1)} = a a^j b a^{-j} a^{-1} = a b^{r^j} a^{-1} = (aba^{-1})^{r^j} = (b^r)^{r^j} = b^{r^{j+1}},$$

como se quería.

Así, en particular, si $j = q$, recordando que $a^q = 1$, de $(*)$ se sigue que

$$b = a^q b a^{-q} = b^{r^q}$$

y por lo tanto $b^{r^q - 1} = 1$ por lo que el orden p de b divide a $r^q - 1$, i.e., $r^q \equiv 1 \pmod p$. □

Ejemplo 6. Si $p > 2$ es un primo, entonces existe un grupo G no abeliano de orden $2p$ ya que $p \equiv 1 \pmod 2$ porque p es impar. Por el teorema anterior

$$G \simeq \langle a, b \mid a^2 = 1 = b^p,\ aba^{-1} = b^r \rangle,$$

donde r es un entero tal que $1 < r < p$ y $r^2 \equiv 1 \pmod p$. Ahora, como $p|(r^2 - 1) = (r-1)(r+1)$, entonces $p|r-1$ ó $p|r+1$. Note que si $p|r-1$, entonces $r \equiv 1 \pmod p$ por lo que $r = 1$, lo cual no puede pasar. Se sigue que $r \equiv -1 \pmod p$ y así

$$aba^{-1} = b^{-1}$$

i.e., $bab = a$ por lo que $G \simeq D_{2p}$ es el grupo diédrico de orden $2p$.

Productos semidirectos y subgrupos de Sylow del grupo simétrico S_n. En esta sección calcularemos los subgrupos de Sylow del grupo simétrico S_n y para hacerlo introduciremos una generalización del concepto de producto directo de dos subgrupos, relajando la hipótesis de que los dos subgrupos sean normales en el grupo grande.

Productos semidirectos. Dados dos subgrupos normales K, Q de un grupo G, tales que $KQ = G$ y $K \cap Q = 1$, se dice que G es *producto directo* de Q y K. Al relajar una de las condiciones, pidiendo que $K \lhd G$ y que $Q \subseteq G$ sólo sea un subgrupo, no necesariamente normal, tales que $K \cap Q = 1$ y $KQ = G$, diremos que G es *producto semidirecto* de K por Q y lo denotaremos mediante

$$G = K \rtimes Q.$$

Puede generalizarse la definición de producto semidirecto en la situación siguiente: si $K \lhd G$ y Q' es un grupo isomorfo a un subgrupo $Q \subseteq G$ y se tiene que $K \cap Q =$

1 y $KQ = G$, también diremos que G es *producto semidirecto* de K por Q' y lo denotamos por $G = K \rtimes Q'$, y esta será la definición que usaremos. En esta situación, si $G = K \rtimes Q$, por el segundo teorema de isomorfismo de Noether, $K \cap Q \lhd Q$ y $Q/(K \cap Q) \simeq KQ/K$ y como $K \cap Q = 1$ y $KQ = G$, entonces $Q \simeq G/K$, es decir, el producto semidirecto $G = K \rtimes Q$ necesariamente es de la forma

$$G = K \rtimes G/K.$$

Ejemplo 7. Si $G = S_n$ y $K = A_n \lhd S_n$, el cociente $S_n/A_n \simeq C(2)$ es un grupo cíclico de orden 2, isomorfo a cualquier subgrupo generado por una transposición, digamos $H = \langle (1,2) \rangle$ y se tiene que $A_n \cap H = 1$ y $S_n = A_n H$, por lo que

$$S_n = A_n \rtimes C(2).$$

Ejemplo 8. Si $G = D_{2n}$, $K = R_n$ (el subgrupo de rotaciones), entonces $R_n \lhd D_{2n}$ tiene índice 2 y así $D_{2n}/R_n \simeq C(2)$, donde $C(2)$ es isomorfo a un subgrupo H de D_{2n} generado por cualquier reflexión. Se tiene que

$$D_{2n} = R_n \rtimes C(2).$$

Note que como R_n es cíclico, un generador es la rotación por el ángulo $2\pi/n$, entonces

$$D_{2n} = C(n) \rtimes C(2).$$

Ejemplo 9. Si $G = S_3$ y $K = \langle (a,b,c) \rangle$ es un subgrupo generado por un 3-ciclo, entonces K tiene orden 3 y $[S_3 : K] = 2$, por lo que $K \lhd S_3$. Si H es un subgrupo de S_3 generado por una transposición (s,t), H es cíclico de orden 2 y se tiene que

$$S_3 = \langle (a,b,c) \rangle \rtimes \langle (s,t) \rangle = C(3) \rtimes C(2).$$

Ejemplo 10. Si $G = \mathbb{Z}/6\mathbb{Z} \simeq C(6)$, observe que $C(3) \simeq \mathbb{Z}/3\mathbb{Z} \subseteq \mathbb{Z}/6\mathbb{Z}$ y $C(2) \simeq \mathbb{Z}/2\mathbb{Z} \subseteq \mathbb{Z}/6\mathbb{Z}$ y se tiene que

$$\mathbb{Z}/6\mathbb{Z} = C(3) \rtimes C(2).$$

Estos dos últimos ejemplos nos permiten observar que, como $S_3 \not\simeq \mathbb{Z}/6\mathbb{Z}$, un producto semidirecto $C(3) \rtimes C(2)$ no está determinado por sus factores $C(3)$ y $C(2)$, a diferencia de lo que sucede con productos directos (vea el ejercicio 11 en el Capítulo 7). Un primer objetivo es ver cómo recuperar un producto semidirecto $G = K \rtimes Q$ a partir de sus subgrupos K y Q. El lema siguiente nos dice que, si $G = K \rtimes Q$, se tiene una *acción* de Q en K que, de alguna forma, describe cómo K es normal en G.

LEMA 9.19. *Supongamos que $G = K \rtimes Q$. Entonces,*

(1) *Se tiene una acción $Q \times K \to K$ dada por $\sigma * k := \sigma k \sigma^{-1}$, a la que se suele denotar por $\sigma * k =: k^\sigma$. Esta acción es lineal en cada una de sus dos variables, i.e.,*

(i) *Si $k, k' \in K$ y $\sigma \in Q$, entonces $(kk')^\sigma = k^\sigma k'^\sigma$.*
(ii) *Si $\sigma, \sigma' \in Q$ y $k \in K$, entonces $k^{(\sigma\sigma')} = (k^{\sigma'})^\sigma$.*

Note el orden de la acción en la notación exponencial, i.e., en la acción de $\sigma\sigma'$ en k, primero actúa σ' y luego actúa σ.

(2) *Si $g = k\sigma$ y $g' = k'\sigma'$ son elementos de $G = KQ$, con $k, k' \in K$ y $\sigma, \sigma' \in Q$, el producto gg' en G está dado por*

$$gg' = (kk'^{\sigma})(\sigma\sigma'),$$

donde k'^{σ} denota la acción de σ en k'.

Demostración. (1): Sólo observamos que, como $K \lhd G$, entonces K es cerrado bajo conjugaciones de G, en particular de Q, y lo demás es el ejemplo 6 del Capítulo 8.

(2): $gg' = (k\sigma)(k'\sigma') = k(\sigma k\sigma^{-1})(\sigma\sigma') = (kk'^{\sigma})(\sigma\sigma')$. □

En el contexto de este lema, diremos que la acción bilineal $Q \times K \to K$ *realiza* al producto semidirecto $G = K \rtimes Q$.

Supongamos ahora que K, Q son dos grupos y que se tiene una acción bilineal de Q en K, $\theta : Q \times K \to K$. Definamos

$$K \rtimes_\theta Q := K \times Q$$

con la operación binaria

$$(\sigma, x) \cdot (\tau, y) := (\sigma\tau^x, xy)$$

donde τ^x denota la acción θ de x en τ, i.e., $\tau^x := \theta(x, \tau)$. Note que, en la notación exponencial, si $x, y \in Q$, $\tau^{xy} = xy * \tau = x * (y * \tau) = (\tau^y)^x$, y si $\sigma, \tau \in K$, entonces $(\sigma\tau)^x = \theta(x, \sigma\tau) = x * (\sigma\tau) = (x\sigma)(x\tau) = \theta(x, \sigma)\theta(x, \tau) = \sigma^x\tau^x$.

TEOREMA 9.20. (1) *$G = K \rtimes_\theta Q$ es un grupo.*

(2) *$K = \{(k, 1) \in K \times Q\} \lhd G$ y $Q = \{(1, x) \in K \times Q\} \subseteq G$ es un subgrupo.*

(3) *$G = K \rtimes Q$ es un producto semidirecto que realiza a θ.*

Demostración. (1): El producto es *asociativo* porque

$$[(k, x)(k', y)](k'', z) = (kk'^x, xy)(k'', z) = (kk'^x k''^{xy}, xyz)$$

y

$$\begin{aligned}(k, x)[(k', y)(k'', z)] &= (k, x)(k'k''^y, yz) = (k(k'k''^y)^x, xyz) \\ &= (kk'^x k''^{xy}), xyz).\end{aligned}$$

El neutro de $K \rtimes_\theta Q$ es $(1, 1)$ y el inverso de (k, x) es $((k^{-1})^{x^{-1}}, x^{-1})$ ya que

$$(k, x)((k^{-1})^{x^{-1}}, x^{-1}) = (k(k^{-1})^{xx^{-1}}, xx^{-1}) = (kk^{-1}, 1) = (1, 1).$$

(2): Si definimos $\pi : G \to Q$ mediante $\pi(k, x) = x$, claramente π es un homomorfismo (ya que la acción θ sólo afecta a la primer coordenada) y $\ker \pi = K$, por lo que $K \lhd G$.

Por otra parte, $Q = \{(1,x) \in K \times Q\} \subseteq G$ es claramente un subgrupo de $K \rtimes_\theta Q$ ya que

$$(1,x)(1,y) = (1 \cdot 1^x, xy) = (1,xy).$$

(3): Es claro que $K \cap Q = \{(1,1)\}$ y $KQ = G$ ya que si $(k,x) \in G$, entonces $(k,1) \in K$ y $(1,x) \in Q$ satisfacen

$$(k,1)(1,x) = (k \cdot 1^1, 1x) = (k,x).$$

Finalmente, para ver que $G = K \rtimes_\theta Q$ realiza a θ, calculamos

$$\begin{aligned}(1,x)(k,1)(1,x)^{-1} &= (1 \cdot k^x, x \cdot 1)(1,x^{-1}) \\ &= (k^x, x)(1,x^{-1}) \\ &= (k^x \cdot 1^x, xx^{-1}) \\ &= (k^x, 1),\end{aligned}$$

es decir, $xkx^{-1} = k^x = x * k$, como se quería. □

El recíproco de este teorema también es válido:

TEOREMA 9.21. *Si $G = K \rtimes Q$ es un producto semidirecto de K por Q, entonces $G \simeq K \rtimes_\theta Q$, para alguna acción θ de Q en K.*

Demostración. Como $G = K \rtimes Q$, por el lema se tiene la acción $\theta : Q \times K \to K$ dada por $\theta(k,x) = k^x = xkx^{-1}$. Ahora, como $G = KQ$ y $K \cap Q = 1$, todo elemento $g \in G$ tiene una descomposición única de la forma $g = kx$ con $k \in K$ y $x \in Q$. El producto de G satisface que, para $g = kx$ y $g' = k'x'$ en G,

$$(*) \qquad gg' = (kx)(k'x') = kk'^x xx'$$

y si definimos $\phi : K \rtimes_\theta Q \to G = K \rtimes Q$ mediante $\phi(k,x) := kx$, la igualdad $(*)$ nos dice que ϕ es un homomorfismo y claramente es biyectivo. □

PROPOSICIÓN 9.22. *$K \rtimes_\theta Q \simeq K \times Q$ si y sólo si la acción θ es trivial, i.e., $k^x = k$ para todo $k \in K$ y $x \in Q$.*

Demostración. Si la acción es trivial, dados $(k,x), (k',x') \in K \rtimes_\theta Q$, su producto es

$$(k,x)(k',x') = (kk'^x, xy) = (kk', xy)$$

el cual es el producto de $K \times Q$. El recíproco es similar. □

Productos corona. Sean A, Q grupos, con Q finito y sea K el producto directo de $|Q|$ copias de A, i.e.,

$$K = \underbrace{A \times \cdots \times A}_{|Q|\text{-copias}}.$$

Podemos pensar a los elementos de K como $|Q|$-adas ordenadas con entradas en A, o mejor aún, como funciones de Q en A, i.e.,

$$K = A^Q = \{f : Q \to A \ : \ f \text{ es una función}\}$$

y por lo tanto el producto en K, coordenada a coordenada, se interpreta como

$$(f \cdot g)(x) = f(x)g(x)$$

para $x \in Q$ y donde pensamos a $f(x)$ como la coordenada x-ésima del vector f.

Para los grupos $K = A^Q$ y Q anteriores, definamos la acción θ de Q en K mediante $\theta(f, y) = f^y$, donde $f^y(x) := f(xy)$, para $f \in K$, $y, x \in Q$. Note que si pensamos a f como un vector con coordenadas $f(x)$ para $x \in Q$,

$$f = (\ldots, f(x), \ldots)$$

entonces $f^y \in K$ es el vector cuyas entradas se obtienen de las del vector f trasladándolas mediante el producto por y a la derecha:

$$f^y = (\ldots, f(xy), \ldots)$$

Podemos entonces definir el producto semidirecto de $K = A^Q$ por Q, al que se llama el *producto corona* de A por Q, y se denota mediante

$$A \wr Q := A^Q \rtimes Q = A^Q \rtimes_\theta Q.$$

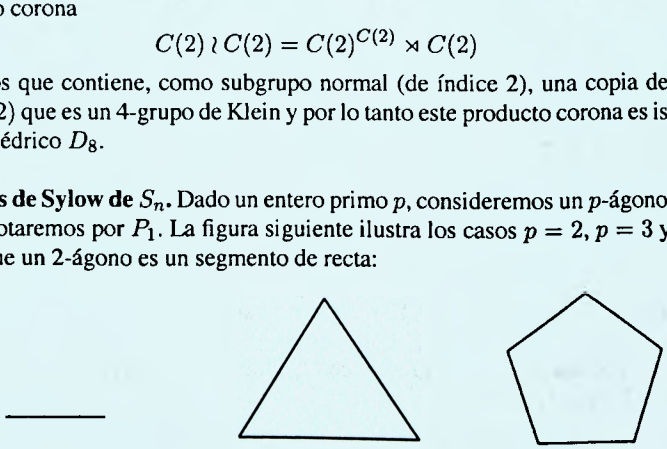
Si los grupos A y Q son finitos, el orden de $A \wr Q$ es $|A \wr Q| = |A^Q \rtimes Q| = |A|^{|Q|}|Q|$.

Ejemplo 11. Si $A = C(2)$ y $Q = C(2)$, entonces $K = C(2) \times C(2) \simeq C(2)^{C(2)}$. Para el producto corona

$$C(2) \wr C(2) = C(2)^{C(2)} \rtimes C(2)$$

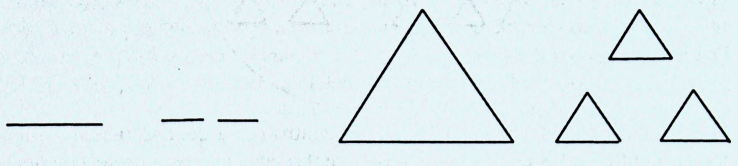
observamos que contiene, como subgrupo normal (de índice 2), una copia del grupo $C(2) \times C(2)$ que es un 4-grupo de Klein y por lo tanto este producto corona es isomorfo al grupo diédrico D_8.

Subgrupos de Sylow de S_n. Dado un entero primo p, consideremos un p-ágono regular al que denotaremos por P_1. La figura siguiente ilustra los casos $p = 2$, $p = 3$ y $p = 5$, notando que un 2-ágono es un segmento de recta:

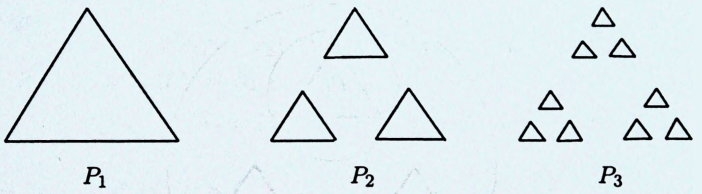


$p = 2$ $p = 3$ $p = 5$

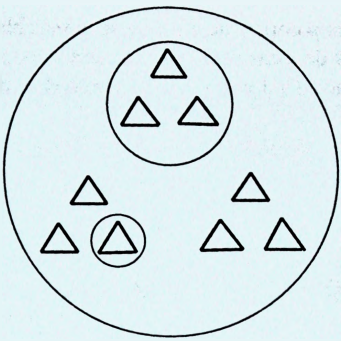
Después, consideremos p copias de P_1, que sean más chicas que P_1 en el sentido que si colocamos cada una de estas copias en los vértices de P_1, éstas no se traslapan ni en los vértices. Llamemos P_2 a esta colección de copias de P_1. La figura siguiente ilustra los casos $p = 2$ y 3:



Luego, consideremos p copias de P_2, que sean más chicas que P_2 en el sentido que si colocamos cada una de estas copias en los vértices de P_2, éstas no se traslapan ni en los vértices. Llamemos P_3 a esta colección de copias de P_2. La figura siguiente ilustra el caso $p = 3$:

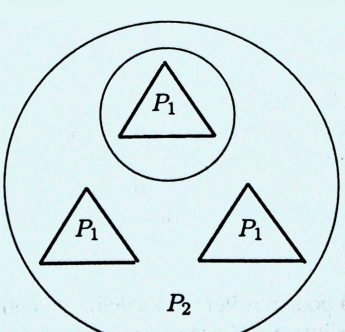


Esta construcción la podemos iterar para definir el polígono P_t, que está dado por p^{t-1} copias de P_1, y nos interesa el subgrupo de simetrías de P_t formado por las rotaciones que lo dejan invariante. Denotemos este grupo por K_t. Por ejemplo, para $p = 3$ y para el polígono P_3, la figura siguiente ilustra algunas de estas simetrías, rotando 120^0 toda la configuración P_3, rotando el P_2 superior 120^0 y rotando 240^0 el P_1 inferior derecho en el P_2 inferior izquierdo, lo cual en la figura lo indicamos por los círculos alrededor de los triángulos correspondientes.



La idea es imaginar una rueda grande dentro de la cual se tienen 3 ruedas más pequeñas dentro de las cuales hay un total de 9 ruedas menores correspondientes a las copias de P_1, y cada una de estas ruedas puede girar independientemente manteniendo las simetrías de los P_j dentro de P_t. Pensando recursivamente, el objetivo es obtener la estructura del grupo de simetrías K_t de P_t usando K_{t-1}, aprovechando que el grupo de simetrías K_1 de P_1 es conocido: es el grupo cíclico de orden p, generado por una rotación por un ángulo de $360/p$ grados.

Veamos en detalle el caso $p = 3$ que estamos ilustrando, para intuir el caso general. En particular, consideremos el grupo K_2 de simetrías de P_2 para $p = 3$ y denotemos por R_1 al subgrupo de simetrías de K_2 que mueven sólo al triángulo P_1 superior y dejan las otras dos copias de P_1 fijas. Así, R_1 consiste de las rotaciones de P_1 por los ángulos 0^0, 120^0 y 240^0:



Similarmente se definen los subgrupos R_2 y R_3, considerando las dos copias inferiores de P_1 en P_2. Note que $R_1 \simeq R_2 \simeq R_3$ son subgrupos isomorfos a K_1. Más aún, como para $i \neq j$, R_i y R_j mueven distintos triángulos, entonces $R_i \cap R_j = 1$ para $i \neq j$. Similarmente, $R_i \cap (R_j \cap R_k) = 1$ para índices distintos, y así $R_1 \times R_2 \times R_3$ es

un subgrupo de K_2 que es isomorfo a $K_1 \times K_1 \times K_1$. Así, un elemento de $R_1 \times R_2 \times R_3$ es una terna (r_1, r_2, r_3) de rotaciones r_i de P_1 por ángulos de 0, 120 ó 240 grados.

Ahora, sea t la rotación por $120 = 360/3$ grados de todo P_3 (la *rueda grande*) y observe que al conjugar

$$t(R_1 \times R_2 \times R_3)t^{-1} = R_1 \times R_2 \times R_3$$

porque, para $(r_1, r_2, r_3) \in R_1 \times R_2 \times R_3$ se tiene que $t(r_1, r_2, r_3)t^{-1}$ actúa en P_2 de la forma siguiente: t^{-1} rota por -120^0 llevando la copia de P_1 arriba, abajo a la izquierda, la de la izquierda abajo a la derecha abajo y la derecha de abajo hacia arriba. Luego, (r_1, r_2, r_3) actúa como sigue: r_3 rota al P_1 de abajo a la izquierda (que solía ser el de arriba), r_2 rota al P_1 de abajo a la derecha (que fue el de abajo a la izquierda), y r_1 rota al P_1 de arriba (que fue el abajo a la derecha). Finalmente, t rota la configuración anterior 120^0. El resultado final es:

$$t(r_1, r_2, r_3)t^{-1} = (r_3, r_1, r_2).$$

En general, para el grupo K_t de simetrías de P_t, sean R_i, $1 \leq i \leq p$, los subgrupos de K_t formado por las rotaciones de las copias i-ésimas de P_{t-1} dentro de P_t y consideremos el producto $R_1 \times \cdots \times R_p \subseteq K_t$. Sea t la rotación de todo P_t por un ángulo de $360/p$ grados. Etiquetemos los P_{t-1} dentro P_t comenzando con el de arriba y yendo en el sentido de las manecillas del reloj como $(1, 2, \ldots, p)$. Entonces la composición $t(r_1, \ldots, r_p)t^{-1}$ actúa como sigue:

$$(1, 2, \ldots, p) \overset{t^{-1}}{\longmapsto} (2, 3, \ldots, p, 1) \overset{(r_1, \ldots, r_p)}{\longmapsto} (r_1(2), r_2(3), \ldots, r_{p-1}(p), r_p(1))$$
$$\overset{t}{\longmapsto} (r_p(1), r_1(2), r_2(3), \ldots, r_{p-1}(p))$$

por lo que

$$t(r_1, \ldots, r_p)t^{-1} = (r_p, r_1, r_2, \ldots, r_{p-1})$$

y así $t(R_1 \times \cdots \times R_p)t^{-1} = R_1 \times \cdots \times R_p$.

PROPOSICIÓN 9.23. (1) $K_t = (R_1 \times \cdots \times R_p)\langle t \rangle$, *donde* $\langle t \rangle$ *es el subgrupo cíclico de orden p generado por t.*

(2) $(R_1 \times \cdots \times R_p) \cap \langle t \rangle = 1$.

(3) $R_1 \times \cdots \times R_p \lhd K_t$.

Por lo tanto, K_t *es el producto semidirecto de* $R_1 \times \cdots \times R_p$ *con* $\langle t \rangle$.

Demostración. Para (1) sólo note que las simetrías rotacionales de P_t se componen de las rotaciones de todo P_t y de las rotaciones independientes de los P_i contenidos en él. Recursivamente se tiene el resultado deseado. Para (2), como $\langle t \rangle = \{1, t, t^2, \ldots, t^{p-1}\}$, note que si $1 \leq i \leq p-1$, t^i mueve un P_{t-1} en otro diferente por lo que $(R_1 \times \cdots \times R_p) \cap \langle t \rangle = 1$. La parte (3) es lo que se demostró arriba, observando que $t^i(R_1 \times \cdots \times R_p)t^{-i} = R_1 \times \cdots \times R_p$. □

Hemos así mostrado que $K_t = (R_1 \times \cdots \times R_p) \rtimes \langle t \rangle$, y como $R_i \simeq K_{t-1}$, entonces $R_1 \times \cdots \times R_p \simeq K_{t-1}^p$ (el producto directo de p copias de K_{t-1}) y por lo tanto

$$K_t = K_{t-1} \wr \langle t \rangle$$

es el *producto corona* de K_{t-1} (rotaciones de P_{n-1}) con el grupo cíclico $\langle t \rangle$.

Ahora, como el grupo K_1 de rotaciones de P_1, es el grupo cíclico $C(p)$ de orden p, generado por una rotación por un ángulo de $360/p$ grados y como $\langle t \rangle \simeq C(p)$, entonces

$$K_2 = K_1 \wr \langle t \rangle = C(p) \wr C(p)$$

y así

$$K_3 = K_2 \wr \langle t \rangle \simeq (C(p) \wr C(p)) \wr C(p)$$

y, recursivamente, obtenemos el grupo K_t de simetrías rotacionales de P_t como el producto corona de t copias de $C(p)$:

$$K_t = (\underbrace{C(p) \wr \cdots \wr C(p)}_{(t-1)\text{-copias}}) \wr C(p).$$

Note ahora que si se numeran los vértices de los polígonos en P_t, que consiste de p^{t-1} copias de un p-ágono regular, se tienen $p(p^{t-1}) = p^t$ vértices, y una simetría rotacional de P_t permuta estos vértices por lo que K_t es un subgrupo del grupo simétrico S_{p^t}. Para calcular el orden de este subgrupo, observe que:

$$|C(p) \wr C(p)| = |C(p)^{C(p)}||C(p)| = p^p p = p^{p+1}$$

$$|(C(p) \wr C(p)) \wr C(p)| = |(C(p) \wr C(p))^{C(p)}||C(p)| = (p^{p+1})^p p = p^{p^2+p+1}$$

$$\vdots$$

$$|(\underbrace{C(p) \wr \cdots \wr C(p)}_{(t-1)\text{-copias}}) \wr C(p)| = |(\underbrace{C(p) \wr \cdots \wr C(p)}_{(t-1)\text{-copias}})^{C(p)}||C(p)|$$

$$= p^{p^{t-1}+p^{t-2}+\cdots+p+1},$$

y veremos que $p^T := p^{p^{t-1}+p^{t-2}+\cdots+p+1}$ es el orden correcto para que este producto corona sea un p-subgrupo de Sylow de S_{p^t}, es decir, mostraremos que p^T es la mayor potencia de p que divide al factorial $p^t!$. Para probar ésto, observemos que dados enteros positivos k, m, si consideramos la pregunta: ¿cuántos enteros entre 1 y m son divisibles por k?, lo que queremos es encontrar los múltiplos de k que hay entre 1 y m, i.e.,

$$1, \ldots, k, \ldots, 2k, \ldots, 3k, \ldots, tk \leq m, \ldots, (t+1)k > m$$

y así la respuesta es: hay t múltiplos de k entre 1 y m; dicho en otras palabras, $t = [m/k]$ es el mayor entero $\leq m/k$. Si ahora pasamos a considerar la pregunta: ¿cuál es la mayor potencia del primo p que divide al factorial $m!$?, por la respuesta a la primer pregunta, de los factores $1, 2, 3, \ldots, (m-1), m$ de $m!$, $[m/p]$ de ellos son divisibles por

p, $[m/p^2]$ de ellos son divisibles por p^2, $[m/p^3]$ de ellos son divisibles por p^3, etcétera, y por lo tanto, si $m! = p^T n$ con $p \nmid n$, entonces los primeros contribuyen el factor $p^{[m/p]}$, los segundos contribuyen el factor $p^{2[m/p^2]}$, pero como un factor divisible por p^2 lo es por p, sólo tomamos una contribución, i.e., $p^{[m/p^2]}$, los terceros contribuyen el factor $p^{3[m/p^3]}$, pero como un factor divisible por p^3 lo es por p^2 y p, sólo tomamos una contribución, i.e., $p^{[m/p^3]}$, etcétera, y por lo tanto el mayor factor p^T en $m!$ es

$$p^T = p^{[m/p]+[m/p^2]+[m/p^3]+\cdots}$$

donde notamos que la suma en el exponente es finita porque $[m/p^k] = 0$ cuando $p^k > m$. En particular, si $m = p^t$, $[p^t/p] = p^{t-1}$, $[p^t/p^2] = p^{t-2}$, etcétera, por lo que en este caso

$$T = p^{t-1} + p^{t-2} + p^{t-3} + \cdots + p + 1$$

y así este p^T es el orden de un p-subgrupo de Sylow del grupo simétrico S_{p^t}, el cual, por la fórmula anterior, coincide con el orden del p-subgrupo

$$\underbrace{(C(p) \wr \cdots \wr C(p))}_{(t-1)\text{-copias}} \wr C(p)$$

de S_{p^t} y por lo tanto este producto corona es un p-subgrupo de Sylow de S_{p^t}.

Usando lo anterior, podemos calcular un p-subgrupo de Sylow de cualquier grupo simétrico S_n, como sigue. Primero escribimos n en base p:

$$n = a_0 + a_1 p + a_2 p^2 + \cdots + a_r p^r$$

con $0 \leq a_i \leq p-1$. Después, partimos el conjunto $\mathbb{I}_n$ en a_0 subconjuntos X_0 con $1 = p^0$ elemento, a_1 subconjuntos X_1 con p elementos, a_2 subconjuntos X_2 con p^2 elementos, etcétera. Cada uno de estos subconjuntos X_i tiene p^i elementos por lo que $S_{X_i} \simeq S_{p^i}$, y por el procedimiento anterior podemos construir un p-subgrupo de Sylow H_i de S_{p^i}. El producto directo de las a_i copias de H_i es un p-subgrupo de Sylow del producto directo de a_i copias de S_{p^i}, (vea el ejercicio 10 de este capítulo) al que denotamos por $S_{p^i}^{a_i}$. Finalmente, el producto directo $H_0^{a_0} \times H_1^{a_1} \times \cdots \times H_r^{a_r}$ es un p-subgrupo de Sylow del producto $S_{p^0}^{a_0} \times S_p^{a_1} \times S_{p^2}^{a_2} \times \cdots \times S_{p^r}^{a_r}$, que es isomorfo a S_n.

Notas. En 1844-46, Cauchy [27, §XII, Théorème V, pág. 280] probó que un grupo finito cuyo orden es divisible por un primo, tiene un elemento de orden ese primo. Ludwig Sylow, en 1872, generalizó el teorema de Cauchy, y los teoremas de Sylow [54] son el punto de partida para iniciar el estudio a profundidad de la estructura de los grupos finitos. Tal ha sido la influencia de los teoremas de Sylow que a lo largo de los años se han producido diferentes demostraciones de los mismos, una tendencia iniciada por Frobenius en [33] (donde además introduce en forma natural los axiomas que definen un grupo abstracto, como observamos en las notas del capítulo 2), y su demostración

usa clases de conjugación, que él define y comienza a estudiar sistemáticamente en este artículo, y la ecuación de clases del grupo. Otra demostración elegante es la de Wielandt [57], que depende de las propiedades de divisibilidad por p de los coeficientes binomiales $\binom{n}{p^k}$. En este capítulo, la demostración que dimos sigue una idea de R. J. Nunke citada en Hungerford [8]. El cálculo de la estructura de los p-subgrupos de Sylow de S_n se debe a Kaloujnine [46], reescrita en [24] en la forma en que la presentamos en este capítulo.

EJERCICIO 1. Demuestre que los 2-subgrupos de Sylow de S_4 son isomorfos a D_8.

EJERCICIO 2. Calcule los 3-subgrupos de Sylow de S_5. Calcule sus 5-subgrupos de Sylow.

EJERCICIO 3. Muestre que los grupos de órdenes 15, 35 y 77 son cíclicos.

EJERCICIO 4. Muestre hay grupos no abelianos de órdenes 55 y 21.

EJERCICIO 5. Demuestre que un 2-subgrupo de Sylow de S_5 es isomorfo a D_8.

EJERCICIO 6. Demuestre que un 2-subgrupo de Sylow de A_5 tiene exactamente 5 conjugados.

EJERCICIO 7. ¿Cuál es la relación entre un 2-subgrupo de Sylow de S_4 y el grupo de simetrías del cuadrado?

EJERCICIO 8. Si G es un grupo de orden 12 y no tiene elementos de orden 2 en su centro, demuestre que $G \simeq A_4$.

EJERCICIO 9. Demuestre que todo grupo de orden $5 \cdot 7 \cdot 13$ es cíclico.

EJERCICIO 10. Sean G', G'' grupos finitos y sea $G = G' \times G''$. Demuestre que los p-subgrupos de Sylow de G son de la forma $H' \times H''$, donde H' y H'' son p-subgrupos de Sylow de G' y G'', respectivamente.

EJERCICIO 11. Calcule los subgrupos de Sylow de $S_3 \times A_4$ y de $S_3 \times C(20)$.

EJERCICIO 12. Si G es un grupo finito de orden $|G| = pqr$, con $p < q < r$ primos, demuestre que G tiene un subgrupo normal de orden qr.

EJERCICIO 13. Si G es un grupo finito de orden $|G| = pqr$, con $p < q < r$ primos, demuestre que el r-subgrupo de Sylow de G es normal en G.

EJERCICIO 14. Sea G un grupo finito y sea P un p-subgrupo de Sylow de G. Demuestre que el normalizador de $N_G(P)$ es igual a $N_G(P)$.

EJERCICIO 15. Sea G un grupo finito y suponga que para cada primo p el grupo G sólo tiene un p-subgrupo de Sylow. Demuestre que G es el producto directo de sus subgrupos de Sylow.

EJERCICIO 16. Si G es un p-grupo finito y $1 \neq H \lhd G$, demuestre que $H \cap Z(G) \neq 1$.

EJERCICIO 17. Sean G un grupo finito y H un subgrupo de G. Demuestre que el número de subgrupos de G conjugados a H es $[G : N_G(H)]$. *Sugerencia*: En la definición de $N_G(H)$, ¿cuál es la órbita de H?

EJERCICIO 18. Si Q es un p-subgrupo normal de un grupo finito G, demuestre que Q está contenido en todos los p-subgrupos de Sylow P de G.

Capítulo **10**

Grupos simples

RECORDEMOS QUE UN GRUPO SIMPLE es un grupo $G \neq 1$ que no tiene subgrupos normales propios. Los ejemplos más sencillos de grupos simples son los grupos cíclicos de orden primo, y éstos son todos los grupos abelianos finitos simples. En este capítulo, y como una aplicación de los teoremas de Sylow, comenzamos mostrando la no existencia de grupos simples de ciertos órdenes pequeños y después obtenemos algunos resultados generales sobre la no existencia de grupos simples de órdenes pq y p^2q, con p y q primos, todo lo anterior como casos especiales de un celebrado teorema de Burnside que dice que si $|G| = p^r q^s$ con $r + s > 1$, entonces G no es simple, cuya demostración requiere resultados no tan elementales y pospondremos su demostración hasta el capítulo 15, como una aplicación de la teoría de caracteres. Al final terminamos mostrando que los grupos alternantes A_n son simples para $n \geq 5$ siendo ésta la primera familia de grupos simples no abelianos que encontraremos. En el capítulo 12 mostraremos otra familia infinita de grupos simples finitos.

Comenzamos con algunas aplicaciones de los teoremas de Sylow para mostrar la no existencia de grupos simples de orden pequeño.

Ejemplo 1. No existe un grupo simple de orden 30. En efecto, supongamos que G es un grupo de orden $30 = 2 \cdot 3 \cdot 5$, cuyos divisores son: 1, 2, 3, 5, 6, 10, 15, 30.

El número n_5 de 5-subgrupos de Sylow de G debe ser un divisor de 30 y además $n_5 \equiv 1$ (mód 5), por lo que las posibilidades para n_5 son 1 y 6. Si $n_5 = 1$ entonces el 5-subgrupo de Sylow sería normal y por lo tanto G no es simple. Probaremos que éste es el caso mostrando que el caso $n_5 = 6$ no puede suceder, pero antes de hacer ésto consideremos el número n_3 de 3-subgrupos de Sylow de G, como $n_3 \equiv 1$ (mód 3), las posibilidades para n_3 son 1 y 10. Si $n_3 = 1$ entonces el 3-subgrupo de Sylow sería normal y por lo tanto G no es simple. Por lo tanto, debemos mostrar que los casos $n_3 = 10$ y $n_5 = 6$ no pueden darse. En efecto, si $n_5 = 6$, entonces los seis 5-subgrupos de Sylow de G contribuyen $6(5-1)$ elementos a G y si $n_3 = 10$ los diez 3-subgrupos de Sylow de G contribuyen $10(3-1)$ elementos a G. Así, con las contribuciones de los 5-subgrupos de Sylow y de los 3-subgrupos de Sylow, y del neutro, G tiene al menos

$6(5-1)+10(3-1)+1=45$ elementos, una contradicción con el orden de G que es 30.

Ejemplo 2. No hay un grupo simple de orden 84. En efecto, supongamos que G es un grupo de orden $84=2^2\cdot 3\cdot 7$, cuyos divisores son: 1, 2, 3, 4, 6, 7, 12, 14, 21, 28, 42, 84.

Ahora, para el número n_7 de 7-subgrupos de Sylow de G, como $n_7\equiv 1$ (mód 7), la única posibilidad para n_7 es 1, por lo que el 7-subgrupo de Sylow es normal y por lo tanto G no es simple.

Ejemplo 3. No existe un grupo simple de orden 12. En efecto, supongamos que G es un grupo de orden $12=2^2\cdot 3$, cuyos divisores son: 1, 2, 3, 4, 6, 12.

El número n_3 de 3-subgrupos de Sylow de G satisface que $n_3\equiv 1$ (mód 3), por lo que las posibilidades para n_3 son 1 y 4. Si $n_3=1$ entonces el 3-subgrupo de Sylow sería normal y por lo tanto G no es simple. Si $n_3=4$, entonces los cuatro 3-subgrupos de Sylow de G contribuyen $4(3-1)=8$ elementos a G, y así los $12-8=4$ elementos restantes sólo pueden formar un único 2-subgrupo de Sylow de G que por lo tanto sería normal por lo que G no puede ser simple.

Este último ejemplo se puede generalizar:

PROPOSICIÓN 10.1. *Si p, q son primos, entonces no existe un grupo simple de orden p^2q.*

Demostración. Si G es abeliano, por el teorema de Cauchy tiene un subgrupo de orden p y éste es normal.

Si G no es abeliano y $p=q$, entonces $|G|=p^3$, por lo que G es un p-grupo y por el lema 9.10 se tiene que $Z(G)\neq 1$ y como $Z(G)\lhd G$, entonces G no es simple.

Si G no es abeliano y $p\neq q$ se tienen dos casos:

CASO 1. Si $q<p$, como por el primer teorema de Sylow G tiene un p-subgrupo de Sylow H_p y como $|H_p|=p^2$, entonces $[G:H_p]=q<p$ y así 9.15 implica que $H_p\lhd G$, por lo que G no es simple.

CASO 2. Si $p<q$, entonces el número n_q de q-subgrupos de Sylow de G divide a $|G|=p^2q$ por lo que sus posibilidades son $1, p, q, p^2, pq, p^2q$, y como $n_q\equiv 1$ (mód q), estas posibilidades se reducen a 1 ó p ó p^2. Ahora, como $p<q$, entonces $p\not\equiv 1$ (mód q), por lo que las posibilidades para n_q se reducen a 1 ó p^2. Si $n_q=1$, entonces el único q-subgrupo de Sylow de G sería normal por lo que G no puede ser simple. Si $n_q=p^2$, los q-subgrupos de Sylow de G contribuyen $p^2(q-1)$ elementos por lo que los $p^2q-p^2(q-1)=p^2$ elementos restantes sólo pueden formar un único p-subgrupo de Sylow de G por lo que éste sería normal y así el grupo G no es simple. □

Observación. En 9.16 probamos que si $|G| = pq$, entonces G no es simple y la proposición anterior nos dice que lo mismo es cierto si $|G| = p^2q$. Los resultados anteriores son casos muy particulares de un celebrado teorema de Burnside, cuya demostración posponemos hasta el capítulo 15, como una aplicación de la teoría de caracteres.

Teorema (Burnside). *Si* $|G| = p^r q^s$ *con* $r + s > 1$, *entonces* G *no es simple.*

El teorema de Burnside es un ejemplo de una familia infinita de grupos no simples. Se conocen varias familias infinitas de grupos simples y a continuación mostraremos que la familia de grupos alternantes A_n son simples si $n \neq 4$. Comenzamos con algunos resultados sobre el centro de estos grupos:

Centros de S_n y A_n. Los grupos S_1, S_2, A_1, A_2 y A_3 son abelianos y por lo tanto son iguales a sus centros.

PROPOSICIÓN 10.2. (1) *Si* $n \geq 3$, *entonces* $Z(S_n) = 1$.

(2) *Si* $n \geq 4$, *entonces* $Z(A_n) = 1$.

Demostración. (1): Dado $\sigma \in S_n$, $\sigma \neq 1$, supongamos que σ ya se ha descompuesto como producto de ciclos disjuntos. Tenemos dos casos:

CASO 1. En la descomposición de σ hay al menos dos ciclos no triviales, digamos

$$\sigma = (x_1, x_2, \ldots)(y_1, y_2, \ldots)\cdots$$

Entonces, como x_1, x_2, y_1, y_2 son diferentes entre sí poniendo $\tau = (x_1, y_1, y_2) \in S_n$, por la proposición 4.11 se tiene que

$$\tau\sigma\tau^{-1} = (y_1, x_2, x_3, \ldots)(y_2, x_1, y_3, \ldots)\cdots \neq \sigma$$

y por lo tanto $\sigma \notin Z(S_n)$.

CASO 2. En la descomposición de σ sólo hay un ciclo no trivial. Se tienen dos subcasos:

SUBCASO (A). En la descomposición de σ sólo hay un ciclo no trivial de longitud ≥ 3, digamos

$$\sigma = (x_1, x_2, x_3, \ldots)$$

Entonces, poniendo $\tau = (x_1, x_2) \in S_n$, por la proposición 4.11 se tiene que

$$\tau\sigma\tau^{-1} = (x_2, x_1, x_3, \ldots) \neq \sigma$$

y por lo tanto $\sigma \notin Z(S_n)$.

SUBCASO (B). En la descomposición de σ sólo hay un ciclo no trivial de longitud < 3, digamos

$$\sigma = (x_1, x_2)$$

y como $n \geq 3$, entonces existe un $x \in \mathbb{I}_n$ distinto de x_1 y x_2, por lo que poniendo $\tau = (x_1, x) \in S_n$, por la proposición 4.11 se tiene que

$$\tau\sigma\tau^{-1} = (x, x_2) \neq \sigma$$

y por lo tanto $\sigma \notin Z(S_n)$.

(2): Dado $\sigma \in A_n$, $\sigma \neq 1$, supongamos que σ ya se ha descompuesto como producto de ciclos disjuntos. Tenemos dos casos:

CASO 1. En la descomposición de σ hay al menos dos ciclos no triviales. Se procede como en el caso 1 del inciso (1), notando que $\tau = (x_1, y_1, y_2) \in A_n$.

CASO 2. En la descomposición de σ sólo hay un ciclo no trivial. Se tienen dos subcasos:

SUBCASO (A). En la descomposición de σ sólo hay un ciclo no trivial de longitud ≥ 4, digamos

$$\sigma = (x_1, x_2, x_3, x_4, \ldots)$$

Entonces, poniendo $\tau = (x_1, x_2)(x_3, x_4) \in A_n$, por la proposición 4.11 se tiene que

$$\tau\sigma\tau^{-1} = (x_2, x_1, x_4, x_3, \ldots) \neq \sigma$$

y por lo tanto $\sigma \notin Z(A_n)$.

SUBCASO (B). En la descomposición de σ sólo hay un ciclo no trivial de longitud < 4. Como $\sigma \in A_n$ debe ser par, la única posibilidad es que sea un 3-ciclo, digamos

$$\sigma = (x_1, x_2, x_3)$$

y como $n \geq 4$, entonces existe un $x \in \mathbb{I}_n$ distinto de x_1, x_2 y x_3, por lo que poniendo $\tau = (x_1, x_2)(x_3, x) \in A_n$, por la proposición 4.11 se tiene que

$$\tau\sigma\tau^{-1} = (x_2, x_1, x) \neq \sigma$$

y por lo tanto $\sigma \notin Z(A_n)$. □

Simplicidad de A_n. Los grupos A_1 y A_3 son triviales y el grupo A_3 es de orden 3, por lo tanto es cíclico de orden primo; así, los grupos A_1, A_2, A_3 son simples. El grupo A_4 no es simple ya que contiene al subgrupo de cuatro elementos, que es normal:

$$V = \{(1),\ (1\ 2)(3\ 4),\ (1\ 3)(2\ 4),\ (1\ 4)(2\ 3)\}.$$

Para demostrar que A_n es simple si $n \geq 5$, usaremos el resultado siguiente:

LEMA 10.3. *Sea $N \lhd A_n$ con $n \geq 5$. Si N contiene un 3-ciclo, entonces $N = A_n$.*

Demostración. Supongamos que $(ijk) \in N$. De acuerdo a los valores de i, j tenemos los casos:

CASO 1. Si $i \neq 2$ y $j \neq 1$, consideremos al elemento $(2\ i)(1\ j) \in A_n$; como $N \lhd A_n$, entonces

$$(*) \qquad (2\ 1\ k) = (2\ i)(1\ j)(ijk)(2\ i)^{-1}(1\ j)^{-1} \in N$$

donde el orden de los inversos es el correcto porque ciclos disjuntos conmutan, y recordando que la inversa de una transposición es ella misma, un cálculo directo da $(*)$. Ahora, como $n \geq 5$, existe un $\ell \in \mathbb{I}_n$ distinto de $1, 2$ y k, y poniendo $\sigma := (1\ 2)(k\ \ell) \in A_n$, conjugando al elemento $(2\ 1\ k) \in N$ por σ, por ejemplo usando 4.11, se tiene que

$$\sigma(2\ 1\ k)\sigma^{-1} = (1\ 2\ \ell) \in N$$

y como $(1\ 2\ k) = (2\ 1\ k)^2 \in N$, entonces N contiene a todos los 3-ciclos de la forma $(1\ 2\ k)$ con $3 \leq k \leq n$, y como A_n está generado por estos 3-ciclos por 4.19, entonces $N = A_n$.

CASO 2. Si $i = 2$ y $j = 1$, entonces N contiene al 3-ciclo $(2\ 1\ k)$ que es $(*)$ del caso 1 y así procedemos como en el caso anterior.

CASO 3. Si $i = 2$ y $j \neq 1$, entonces $(2\ j\ k) \in N$ y para el elemento $(1\ j)(k\ j) \in A_n$ se tiene que

$$(1\ 2\ k) = (2\ k\ j) = (1\ j)(k\ j)(2\ j\ k)(1\ j)^{-1}(k\ j)^{-1} \in N$$

por lo que N contiene a los 3-ciclos $(1\ 2\ k)$ y así $N = A_n$.

CASO 4. Si $i \neq 2$ y $j = 1$, entonces $(i\ 1\ k) \in N$ y para el elemento $(2\ i)(1\ k) \in A_n$ se tiene que

$$(1\ 2\ k) = (k\ 1\ 2) = (2\ i)(1\ k)(i\ 1\ k)(2\ i)^{-1}(1\ k)^{-1} \in N$$

por lo que N contiene a los 3-ciclos $(1\ 2\ k)$ y así $N = A_n$. □

TEOREMA 10.4. *A_n es simple para todo $n \geq 5$.*

Demostración. Sea $N \lhd A_n$, con $n \geq 5$. Si $N \neq 1$, mostraremos que $N = A_n$, y por el lema anterior es suficiente mostrar que N contiene un 3-ciclo. Para ésto, escojamos un $\sigma \in N$, $\sigma \neq 1$, tal que σ deje fijos un número máximo de los elementos de $\mathbb{I}_n$. Si σ es un 3-ciclo ya acabamos. Si σ no fuera un 3-ciclo, consideremos la descomposición de σ en producto de ciclos disjuntos. Hay dos casos a considerar:

CASO 1. σ contiene un ciclo de longitud ≥ 3. Como σ no es un 3-ciclo, entonces mueve al menos a 4 elementos de $\mathbb{I}_n$, i.e., debe ser de la forma

$$\sigma = (i\ j\ k \cdots)(\cdots)\cdots$$

Más aún, σ no puede ser de la forma $\sigma = (i\ j\ k\ \ell)$ ya que éste es un 4-ciclo y por lo tanto es una permutación impar. Se sigue que σ debe mover al menos otro elemento

$m \in \mathbb{I}_n$ distinto de i, j, k, ℓ. Sea $g = (k\ \ell\ m) \in A_n$. Entonces, $\tau := g\sigma g^{-1} \in N$ y τ tiene la misma estructura cíclica que σ y se obtiene aplicando g a los elementos de σ, por lo que

$$\tau = g\sigma g^{-1} = (g(i)\ g(j)\ g(k)\cdots)(\cdots)\cdots = (i\ j\ \ell\cdots)(\cdots)\cdots \neq \sigma$$

Ahora, si r es distinto de i, j, k, ℓ, m y si $\sigma(r) = r$, entonces $\tau(r) = r$ ya que $\tau = g\sigma g^{-1}$ se obtiene aplicando g a los elementos de los ciclos de σ y $g = (k\ \ell\ m)$ no mueve al r, por lo que $\tau(r) = g\sigma g^{-1}(r) = \sigma(r) = r$. Se sigue que $\sigma^{-1}\tau \in N$ es tal que $\sigma^{-1}\tau \neq \mathrm{id}$ (porque $\sigma \neq \tau$) y para todo r distinto de i, j, k, ℓ, m (que son movidos por σ) se tiene que $\sigma^{-1}\tau(r) = r$, y como además $\sigma^{-1}\tau(i) = \sigma^{-1}(j) = i$, entonces $\sigma^{-1}\tau \in N$ no es la identidad y tiene más puntos fijos que σ, en contradicción con la condición de maximalidad con la que se eligió a σ. Se sigue que este caso no se puede dar.

CASO 2. σ contiene al menos dos 2-ciclos distintos, digamos

$$\sigma = (i\ j)(k\ \ell)\cdots$$

Sea $m \in \mathbb{I}_n$ distinto de i, j, k, ℓ y pongamos $g := (k\ \ell\ m) \in A_n$. Entonces

$$\tau := g\sigma g^{-1} = (g(i)\ g(j))(g(k)\ g(\ell))\cdots = (i\ j)(\ell\ m)\cdots$$

está en N y es distinta de σ por lo que $\sigma^{-1}\tau \in N$ no es la identidad. Observe que $\sigma^{-1}\tau$ deja fijos a todos los elementos r (distintos de i, j, k, ℓ, m) que están fijos bajo σ y además, aunque σ pueda fijar al m a pesar de que $\sigma^{-1}\tau$ no fija al m ya que $\sigma^{-1}\tau(m) = \sigma^{-1}(\ell) = k$, notamos que $\sigma^{-1}\tau$ fija a i y j, por lo que $\sigma^{-1}\tau \in N$ tiene más puntos fijos que σ, lo cual es una contradicción. Se sigue que este caso tampoco se puede dar. □

El teorema anterior nos da otro contraejemplo al teorema de Lagrange:

Ejemplo 4. El grupo A_5 tiene orden 60 pero no tiene un subgrupo H de orden 30, ya que si lo tuviera, H tendría índice 2 en A_5 por lo que sería normal, en contradicción con la simplicidad de A_5.

Notas. Los grupos simples finitos son como los ladrillos a partir de los cuales se pueden construir todos los grupos finitos, como lo expresa de alguna forma el teorema de Jordan-Hölder (vea el teorema 11.2 y la nota 7 del capítulo siguiente), y así, clasificar y determinar todos los grupos simples finitos es un objetivo importante de la teoría de grupos.

En su tratado, [11], Jordan enfatiza la distinción que hizo Galois [40] entre grupos simples y *grupos compuestos*, i.e., no simples, necesaria para su caracterización de ecuaciones polinomiales solubles por radicales (definiendo de paso los *grupos solubles* (vea las notas al final del capítulo siguiente)). En este tratado, Jordan comienza la clasificación de los grupos finitos simples (alternantes A_n para $n \geq 5$ y casi todos los grupos lineales proyectivos sobre campos finitos de cardinalidad prima (ver el capítulo

12). Es hasta 1892 cuando Hölder estudia por primera vez grupos simples en forma abstracta y al principio de su artículo [43] escribe:

> «Sería de gran interés si fuera posible dar un panorama de toda la familia de grupos finitos simples.»

Este podría ser considerado el nacimiento del programa cuya meta principal era clasificar y determinar todos los grupos simples finitos, y en este artículo señero de Hölder, él mismo clasifica todos los grupos simples de órdenes hasta 200. Esta cota fue aumentada paulatinamente, usando en las demostraciones las únicas herramientas disponibles hasta entonces, a saber los teoremas de Sylow, hasta que Frobenius y Burnside introdujeron la teoría de caracteres en el arsenal.

A finales de los años 1970 y a principios de la década de 1980, se anunció la conclusión de la clasificación de los grupos finitos simples y según ésto, se tienen las cuatro familias infinitas de grupos simples finitos siguientes: *grupos cíclicos de orden primo*, los *grupos alternantes* A_n con $n \neq 4$, los *grupos lineales clásicos sobre un campo finito* (proyectivos lineales especiales, proyectivos simplécticos unitarios, proyectivos ortogonales, proyectivos unitarios especiales) y *grupos de Chevalley torcidos*. Además de estas familias, se tienen 26 grupos simples finitos que no pertenecen a familia alguna y se les conoce como *grupos esporádicos*, 5 de los cuales fueron descubiertos por Mathieu hacia 1860 y los otros 21 fueron encontrados entre 1965 y 1975. En los años siguientes al anuncio de la completación del programa de la clasificación de los grupos simples finitos se han venido publicando los artículos donde se detalla la clasificación, pero hasta la fecha esto no ha sido concluido. De hecho, algunos matemáticos todavía se mantienen escépticos con respecto a la pretendida conclusión del programa, aunque la mayoría de los algebristas dedicados a la teoría de grupos considera que el programa esencialmente está concluido y sólo es materia de tiempo para que las publicaciones asociadas aparezcan.

EJERCICIO 1. Demuestre que no existen grupos simples no abelianos de orden 28, 36, 56, y 80.

EJERCICIO 2. Calcule el centro del grupo diédrico D_{2n}.

EJERCICIO 3. Demuestre que el homomorfismo $c : G \to \mathrm{Aut}(G)$ dado por $c(\tau)(\sigma) := \tau\sigma\tau^{-1}$ es inyectivo si

(i) $G = S_n$ y $n \geq 3$.
(ii) $G = A_n$ y $n \geq 4$.

EJERCICIO 4. Demuestre que A_5 no tiene subgrupos de orden 15.

EJERCICIO 5. Demuestre que si G es un grupo de orden 12 distinto de A_4, entonces G tiene elementos de orden 6.

EJERCICIO 6. Demuestre que si $n \geq 5$, entonces todos los 3-ciclos de A_n son conjugados del 3-ciclo (1 2 3). Use lo anterior para dar otra demostración del lema 10.3.

Capítulo 11

Grupos solubles

HASTA AHORA, DESPUÉS DE DAR ejemplos de grupos, subgrupos, cocientes y homomorfismos, el primer teorema genérico sobre grupos finitos que probamos es el teorema de Lagrange, el cual restringe el orden de los subgrupos que un grupo finito dado puede tener. Después, los teoremas de Sylow, recíprocos parciales del teorema de Lagrange, garantizan la existencia de ciertos subgrupos de G y nos dan una familia de subgrupos, los p-subgrupos de Sylow de G, donde cada miembro de la familia es conjugado de los otros y consecuentemente todos los miembros de la familia tienen el mismo orden. En este capítulo introducimos la noción de *serie normal* de un grupo (finito) G que nos permitirá estudiar familias de subgrupos de G de órdenes distintos. Junto con la anterior se definen y prueban algunas propiedades básicas de los *grupos solubles*. Estos grupos (y su nombre) aparecieron en el estudio de la solubilidad por radicales de ecuaciones polinomiales, y aparte de su interés en este contexto juegan un papel importante en la teoría de grupos y la aritmética.

Si G es cualquier grupo, una *serie normal* de G es una cadena de subgrupos

$$(*) \qquad G =: G_0 \supseteq G_1 \supseteq G_2 \supseteq \cdots \supseteq G_n = \{e\}$$

tal que $G_{i+1} \lhd G_i$ para toda i. Los *cocientes de la serie* son los grupos G_i/G_{i+1} para $0 \leq i < n$ y la *longitud de la serie* es el número de inclusiones estrictas.

Note que no se está pidiendo que $G_i \lhd G$ ya que, en general, la normalidad no es transitiva.

Una serie normal de un grupo G

$$G =: G_0 \supseteq G_1 \supseteq G_2 \supseteq \cdots \supseteq G_n = 1$$

se dice que es una *serie de composición* si cada G_{i+1} es un subgrupo normal máximo de G_i ó si $G_{i+1} = G_i$. Recuerde que un subgrupo normal $H \lhd G$ se dice que es máximo si no existe otro subgrupo normal $K \lhd G$ entre H y G, i.e., tal que $H \subsetneq K \subsetneq G$. Por el teorema de correspondencia $H \lhd G$ es un subgrupo normal máximo si y sólo si G/H no tiene subgrupos normales propios, i.e., si y sólo si G/H es simple. Así, la serie $(*)$ es una serie de composición de G si y sólo si cada cociente G_i/G_{i+1} es simple o trivial.

Observación. Si G es un grupo finito no simple, entonces G tiene subgrupos normales N propios, i.e., tales que $1 \subsetneq N \subsetneq G$ y así G tiene subgrupos normales máximos ya que si H es máximo ya acabamos; si $H \lhd G$ no es máximo entonces G/H no es simple y así tiene un subgrupo normal propio que bajo el teorema de correspondencia está asociado a un subgrupo normal $K \lhd G$ tal que $H \subsetneq K \subsetneq G$. Si K es máximo ya acabamos, si no procedemos como antes y el proceso termina en un número finito de pasos ya que G es finito.

LEMA 11.1. *Si G es un grupo finito, entonces G tiene una serie de composición.*

Demostración. Si G es simple entonces $1 \lhd G$ es una serie de composición de G. Si G no es simple, por la observación anterior G tiene un subgrupo normal máximo $H_1 \lhd G$. Si H_1 es máximo entonces $1 \lhd H_1 \lhd G$ es una serie de composición de G. Si H_1 no es simple procedemos como antes. Como G es finito el proceso anterior termina en un número finito de pasos. □

Si

$$G =: G_0 \supseteq G_1 \supseteq G_2 \supseteq \cdots \supseteq G_m = 1$$

y

$$G =: G'_0 \supseteq G'_1 \supseteq G'_2 \supseteq \cdots \supseteq G'_n = 1$$

son dos series normales de un grupo G, diremos que son *equivalentes* si existe una biyección entre las familias de grupos cociente $\{G_{i+1}/G_i\}$ y $\{G'_{i+1}/G'_i\}$ tal que los grupos cociente correspondientes son isomorfos. Es claro que series equivalentes tienen la misma longitud.

Ejemplo 1. Para el grupo cíclico $G = C(30)$ de orden 30, se tienen las series de composición

$$G = C(30) \supset C(6) \supset C(3) \supset 1$$

y

$$G = C(30) \supset C(10) \supset C(2) \supset 1$$

con grupos cociente

$$\{C(5), C(2), C(3)\} \quad \text{y} \quad \{C(3), C(5), C(2)\}$$

respectivamente, y por lo tanto las series son equivalentes.

TEOREMA 11.2 (Jordan-Hölder). *Cualesquiera dos series de composición de un grupo finito G son equivalentes.*

Demostración. Por inducción sobre el orden $n = |G|$ de G. Si $n = 2$ la única serie de composición de G es $G \supset 1$ y no hay nada que probar. Supongamos ahora que el teorema es válido para grupos de orden menor que n y sea G de orden n. Si G es

simple, la única serie de composición de G es $G \supset 1$ y el teorema es válido en este caso. Si G no es simple consideremos dos series de composición de G:

$$G =: H_0 \supseteq H_1 \supseteq H_2 \supseteq \cdots \supseteq H_r = 1 \tag{1}$$

y

$$G =: K_0 \supseteq K_1 \supseteq K_2 \supseteq \cdots \supseteq K_t = 1 \tag{2}$$

y distingamos los casos siguientes:

CASO 1. Si $H_1 = K_1$, las dos series de composición obtenidas de (1) y (2) eliminando al grupo G son equivalentes por la hipótesis de inducción aplicada al grupo $H_1 = K_1$, y como $H_0/H_1 = K_0/K_1$, entonces las series (1) y (2) también son equivalentes.

CASO 2. Si $H_1 \neq K_1$, como ambos subgrupos son normales en G entonces $H_1K_1 \lhd G$ y como $H_1 \neq K_1$ entonces $H_1 \subsetneq H_1K_1$ y ya que H_1 es subgrupo normal máximo de G se debe entonces tener que $H_1K_1 = G$. Pongamos ahora $L_1 := H_1 \cap K_1$. Por el segundo teorema de isomorfismo de Noether

$$G/H_1 = H_1K_1/H_1 \simeq K_1/(H_1 \cap K_1) = K_1/L_1 \tag{3}$$

y

$$G/K_1 = H_1K_1/K_1 \simeq H_1/(H_1 \cap K_1) = H_1/L_1 \tag{4}$$

y por lo tanto K_1/L_1 y H_1/L_1 son simples puesto que G/H_1 y G/K_1 lo son. Sea $L_1 \supset L_2 \supset \cdots \supset L_s = 1$ una serie de composición de L_1. Como $H_1 \supset L_1$ y $K_1 \supset L_1$, se tienen las series de composición de G:

$$G \supseteq H_1 \supseteq L_1 \supseteq L_2 \supseteq \cdots \supseteq L_s = 1 \tag{5}$$

y

$$G \supseteq K_1 \supseteq L_1 \supseteq L_2 \supseteq \cdots \supseteq L_s = 1 \tag{6}$$

ya que H_1/L_1 y K_1/L_1 son simples. Los grupos cociente de (5) y (6) son

$$G/H_1, H_1/L_1, L_1/L_2, \ldots, L_s$$

y

$$G/K_1, K_1/L_1, L_1/L_2, \ldots, L_s$$

y así, por (3) y (4) las series (5) y (6) son equivalentes ya que salvo la permutación de los dos primeros grupos de la izquierda, los demás son iguales.

Finalmente, las series de H_1 que se obtienen de (1) y (5) son equivalentes por hipótesis de inducción. Análogamente las series de K_1 que se obtienen de (2) y (6) también son equivalentes. Se sigue que las series de H_1 y K_1 que se obtienen de (1) y (2) son equivalentes y de (3) y (4) se sigue que (1) y (2) son equivalentes también. □

Grupos solubles. Un grupo G finito es *soluble* si tiene una serie normal cuyos cocientes G_i/G_{i+1} son abelianos para $0 \leq i \leq n-1$.

Ejemplo 2. Todo grupo abeliano G es soluble, ya que la serie

$$1 \lhd G$$

satisface la definición.

Ejemplo 3. Un grupo finito simple no abeliano no es soluble ya que su única serie normal es de la forma $1 \lhd G$ y el cociente $G/1 \simeq G$ no es abeliano.

Ejemplo 4. Si p es un primo, recordemos que un p-grupo finito es un grupo cuyo orden es una potencia de p.

PROPOSICIÓN 11.3. *Todo p-grupo finito es soluble. En otras palabras, si G es un grupo de orden p^n, entonces existe una sucesión de subgrupos*

$$1 = G_0 \subseteq G_1 \subseteq \cdots \subseteq G_n = G$$

tales que G_i es normal en G_{i+1}, $|G_i| = p^i$ con $1 \leq i \leq n$ y los cocientes G_{i+1}/G_i son cíclicos de orden p.

Demostración. Por inducción sobre n. Si $n = 0$ es claro. Si $n \geq 1$ entonces, por el lema 9.10, $Z(G) \neq 1$ y como $|Z(G)|$ divide a $|G| = p^n$ entonces $|Z(G)| = p^m$ con $1 \leq m \leq n$. Además, $Z(G)$ abeliano de orden p^m implica que $Z(G)$ tiene un elemento σ de orden p. Sea C el grupo cíclico generado por σ. Entonces así $|C| = p$ y $C \subseteq Z(G)$, y por lo tanto C es normal en G y G/C es un p-grupo de orden p^{n-1}. Por hipótesis de inducción existe una sucesión de subgrupos

$$1 = C/C = G_1/C \lhd \cdots \lhd G_n/C = G/C,$$

donde $|(G_i/C)| = p^{i-1}$ y por lo tanto $G_i = p^{i-1}|C| = p^{i-1}p = p^i$, y $G_i/C \lhd G_{i+1}/C$, lo cual implica que $G_i \lhd G_{i+1}$. Si entonces ponemos $G_0 = 1$ se tiene la serie normal deseada para G y como los cocientes G_{i+1}/G_i tienen orden p y por lo tanto son cíclicos, se sigue que G es soluble. □

Ejemplo 5. Si p y q son primos, cualquier grupo G de orden pq es soluble. En efecto, si $p = q$ entonces G es un p-grupo y así es soluble por la proposición anterior. Si $p \neq q$, podemos suponer que $p > q$ y por el primer teorema de Sylow G tiene un p-subgrupo de Sylow H_p cuyo índice es $[G : H_p] = q < p$ y así por la proposición 9.15, $H_p \lhd G$ y el cociente G/H_p es cíclico de orden q. Se tienen así la serie de composición $1 \subsetneq H_p \subsetneq G$.

Ejemplo 6. Si p y q son primos, cualquier grupo G de orden p^2q es soluble. En efecto, si $p = q$, entonces G es un p-grupo y así es soluble. Si $p \neq q$, tenemos dos casos:

CASO 1. $p > q$. Por el primer teorema de Sylow G tiene un p-subgrupo de Sylow H_p de índice $q < p$ en G y así por 9.15, H_p es normal en G y el cociente G/H_p es cíclico de orden p. Más áun, el grupo H_p es un p-grupo de orden p^2 y así es soluble por la proposición anterior. La serie de composición para H_p se puede extender a una serie

de composición para G simplemente añadiendo G a la serie de H_p y como el cociente G/H_p es cíclico, se tiene entonces una serie de composición de G con cocientes abelianos y por lo tanto G es soluble.

CASO 2. $p < q$. Por Sylow, G tiene un q-subgrupo de Sylow H_q. Ahora, como $1 < p < q$, entonces $p \not\equiv 1$ (mód q) y así el número n_q de q-subgrupos de Sylow de G sólo puede ser 1 ó p^2 (de los divisores de p^2q). Si $n_q = 1$, entonces $H_q \lhd G$ y el cociente G/H_q es de orden p^2 y por lo tanto abeliano por 9.12. Ahora, como H_q es un q-grupo, entonces es soluble por la proposición anterior. Se sigue que G es soluble, como en el caso anterior. Si $n_q = p^2$, como los q-subgrupos de Sylow de G comparten sólo al 1, quitando a éste tienen $p^2(q-1)$ elementos y así los elementos de G que no están en estos q-subgrupos de Sylow son $p^2q - p^2(q-1) = p^2$ y por lo tanto sólo pueden formar un único p-subgrupo de Sylow H_p de G que debe ser entonces normal y el cociente G/H_p tiene orden q y así es cíclico. Como H_p es un p-grupo, es soluble. Se sigue que G es soluble, como en el caso anterior.

Observación. Los dos ejemplos anteriores son casos muy particulares de un celebrado teorema de Burnside, cuya demostración daremos en el capítulo 15, como una aplicación de la teoría de caracteres:

Teorema B. (Burnside). *Si* $|G| = p^r q^s$, *entonces* G *es soluble.*

Esta formulación del teorema de Burnside es equivalente a la dada en el capítulo anterior:

Teorema A. (Burnside). *Si* $|G| = p^r q^s$ *con* $r + s > 1$, *entonces* G *no es simple.*

En efecto, supongamos que el teorema B es cierto. Si G es abeliano, claramente no es simple (porque tiene orden $p^r q^s$ con $r + s > 1$ y por lo tanto tiene un subgrupo propio). Si G no es abeliano, la serie normal $1 \lhd G$ no tiene cociente abeliano y como G es soluble por hipótesis, entonces tiene una serie normal con cocientes abelianos y por lo tanto G debe tener un subgroupo normal propio y así no es simple.

Recíprocamente, supongamos que el teorema A es cierto. Usaremos inducción sobre $|G|$. Como G no es simple, entonces contiene un subgrupo normal propio $H \lhd G$ y así $1 < |H| < |G|$ y como $|H|$ divide a $|G| = p^r q^s$, entonces los órdenes de H y de G/H son de la forma $p^a q^b$. Si $a + b \leq 1$ entonces H es un p-grupo (ó un q-grupo) y por lo tanto es soluble. Si $a + b > 1$, por hipótesis de inducción H es soluble. Lo mismo pasa para G/H. Hemos así mostrado que H y G/H son solubles. Por 11.6(3) se sigue que G es soluble.

Ejemplo 7. El grupo simétrico $G = S_3$ es soluble, mediante la serie

$$1 = G_0 \subseteq G_1 \subseteq G_2 := S_3,$$

donde $G_1 = \{1, (1,2,3), (1,3,2)\}$, ya que es claro que $G_1 \lhd S_3$, y el cociente S_3/G_1 tiene orden $|S_3|/|G_1| = 3!/3 = 2$ y por lo tanto es abeliano, y similarmente $G_1/1 \simeq G_1$ tiene orden 3 y así es abeliano.

Ejemplo 8. El grupo simétrico $G = S_4$ es soluble, mediante la serie

$$1 = G_0 \subseteq G_1 \subseteq G_2 \subseteq S_4,$$

donde $G_2 = A_4$ es el grupo alternante de cuatro elementos, y $G_1 = V$ es el grupo de 4 elementos de Klein (que es abeliano),

$$V = \{1, (12)(34), (13)(24), (14)(23)\}.$$

Después de probar algunas propiedades de los grupos solubles, mostraremos que para $n \geq 5$ el grupo simétrico S_n no es soluble.

Comenzamos con una caracterización de grupos solubles: dado un grupo G, sea

$$G^{(1)} := [G, G]$$

el subgrupo de G generado por los conmutadores $aba^{-1}b^{-1}$ con $a, b \in G$. $[G : G]$ es el *subgrupo conmutador* de G, vea el Capítulo 5, antes de la proposición 5.15.

LEMA 11.4. *Sea G un grupo. Entonces,*

(1) *$G^{(1)}$ es un subgrupo normal de G.*

(2) *El grupo cociente $G/G^{(1)}$ es abeliano.*

(3) *Si $M \lhd G$ es un subgrupo normal tal que G/M es abeliano, entonces $G^{(1)} \subseteq M$.*

Demostración. (1) Es la proposición 5.15.

(2) Dados $a \cdot G^{(1)}, b \cdot G^{(1)} \in G_1/G^{(1)}$ con $a, b \in G$, se tiene que

$$\begin{aligned}
(a \cdot G^{(1)}) \cdot (b \cdot G^{(1)}) &= (ab)G^{(1)} && \text{por definición de producto} \\
&= (ab)(b^{-1}a^{-1}ba)G^{(1)} && \text{ya que } b^{-1}a^{-1}ba \in G^{(1)} \\
&= (ba)G^{(1)} \\
&= (b \cdot G^{(1)})(a \cdot G^{(1)}).
\end{aligned}$$

(3) Mostraremos que todos los generadores $aba^{-1}b^{-1}$ de $G^{(1)}$ están en M. En efecto, para el generador $aba^{-1}b^{-1}$ de $G^{(1)}$, como G/M es abeliano

$$abM = baM$$

y así $aba^{-1}b^{-1} = ab(ba)^{-1} \in M$. □

Como $G^{(1)}$ es un grupo también, podemos considerar su subgrupo conmutador

$$G^{(2)} := [G^{(1)}, G^{(1)}],$$

y en general, iterar el proceso anterior obteniendo una cadena de subgrupos de G:

$$(*) \qquad G \supseteq G^{(1)} \supseteq G^{(2)} \supseteq \cdots \supseteq G^{(i)} \supseteq \cdots$$

donde $G^{(i)} := [G^{(i-1)}, G^{(i-1)}]$ y además (poniendo $G^{(0)} := G$), por el lema anterior se tiene que:

(i) $G^{(i)} \lhd G^{(i-1)}$ para todo $i \geq 1$.
(ii) De hecho, $G^{(i)} \lhd G$ para toda $i \geq 0$.
(iii) Los cocientes $G^{(i)}/G^{(i+1)}$ son abelianos para toda $i \geq 0$.

PROPOSICIÓN 11.5. *Un grupo G es soluble si y sólo si $G^{(n)} = 1$ para algún entero n.*

DEMOSTRACIÓN. Si $G^{(n)} = 1$, la cadena $(*)$ es finita

$$1 = G^{(n)} \subseteq G^{(n-1)} \subseteq \cdots \subseteq G^{(1)} \subseteq G^{(0)} = G$$

y es tal que cada $G^{(i+1)} \lhd G^{(i)}$ y los cocientes $G^{(i)}/G^{(i+1)}$ son abelianos. Se sigue que G es soluble.

Recíprocamente, si G es soluble, se tiene una serie

$$1 = G_0 \subseteq G_1 \subseteq \cdots \subseteq G_n = G$$

donde cada $G_i \lhd G_{i+1}$ y los cocientes G_{i+1}/G_i son abelianos. Entonces, del lema (11.4)(3) se tiene que $[G_{i+1}, G_{i+1}] \subseteq G_i$, y así

$$\begin{aligned} G^{(1)} &:= [G, G] = [G_n, G_n] \subseteq G_{n-1} \\ G^{(2)} &:= [G^{(1)}, G^{(1)}] \subseteq [G_{n-1}, G_{n-1}] \subseteq G_{n-2} \\ &\vdots \\ G^{(n)} &:= [G^{(n-1)}, G^{(n-1)}] \subseteq [G_1, G_1] \subseteq G_0 = 1 \end{aligned}$$

i.e., $G^{(n)} = 1$. □

TEOREMA 11.6. *Sea G un grupo. Entonces,*

(1) *Si $H \subseteq G$ es un subgrupo y G es soluble, entonces H es soluble.*

(2) *Si $H \lhd G$ y G es soluble, entonces G/H es soluble.*

(3) *Si $H \lhd G$ es tal que H y G/H son solubles, entonces G es soluble.*

Demostración. (1) Si $G^{(n)} = 1$, como $H^{(n)} \subseteq G^{(n)} = 1$, entonces $H^{(n)} = 1$.

(2) El homomorfismo canónico $G \to G/H$ induce homomorfismos suprayectivos $G^{(m)} \to (G/H)^{(m)}$, y así, si $G^{(n)} = 1$ entonces $(G/H)^{(n)} = 1$.

(3) Como G/H es soluble, existe m tal que $G^{(m)} \subseteq H$ y como H es soluble existe n tal que $H^{(n)} = 1$, y así $G^{(m+n)} = 1$. □

Observación. Un grupo G se dice que es *extensión de un grupo N por un grupo M*, si G tiene un subgrupo normal $H \lhd G$ isomorfo a N y tal que el cociente G/H es isomorfo a M. Se suele usar la notación

$$\begin{array}{ccccccccc} 1 & \to & H & \hookrightarrow & G & \to & G/H & \to & 1 \\ & & \wr & & & & \wr & & \\ & & N & & & & M & & \end{array}$$

Con esta notación, el teorema previo nos dice que la clase $\mathcal{S}$ de grupos solubles es cerrada bajo subgrupos, cocientes y extensiones. Nótese que la clase $\mathcal{A}$ de grupos abelianos es obviamente cerrada bajo subgrupos y cocientes, pero no lo es bajo extensiones, por ejemplo, el grupo $G = S_3$ tiene el subgrupo normal $H = A_3$ que es cíclico (y así, abeliano) con cociente S_3/A_3 cíclico de orden 2 (y así abeliano), y sin embargo S_3 *no* es abeliano. En este sentido, los grupos solubles se comportan mejor que los abelianos. El lema siguiente nos servirá para probar que los grupos simétricos S_n, $n \geq 5$, no son solubles. Note que en los ejemplos 7 y 8 mostramos que S_3 y S_4 son solubles y obviamente S_1 y S_2 también son solubles ya que son abelianos.

LEMA 11.7. *Sean $n \geq 5$ y $G = S_n$ el grupo simétrico en n letras. Entonces, los grupos conmutadores $G^{(k)}$ de G, $k \geq 1$, contienen todos los 3-ciclos de S_n.*

Demostración. Por la observación (ii) después de (11.4) se tiene que si $N \lhd G$ entonces $N^{(1)} = [N, N] \lhd G$.

Probaremos primero que si $N \lhd G = S_n$, $n \geq 5$, contiene a todos los 3-ciclos de S_n entonces $N^{(1)} = [N, N]$ también contiene a todos los 3-ciclos de S_n.

En efecto, si a, b, c, d, e son 5 letras distintas (aquí es donde usamos que $n \geq 5$), como N contiene a todos los 3-ciclos, entonces $\sigma = (abc)$ y $\tau = (ade)$ están en N, y por lo tanto su conmutador está en $N^{(1)}$:

$$\sigma\tau\sigma^{-1} = (abc)(ade)(cba)(eda) = (abd) \in N^{(1)}.$$

Y como $N^{(1)} \lhd S_n$, para todo $\pi \in S_n$ se tiene que

$$\pi(abd)\pi^{-1} \in N^{(1)}.$$

En particular, para $\pi \in S_n$ tal que $\pi(a) = r$, $\pi(b) = s$, $\pi(d) = t$, donde r, s, t son tres enteros (entre 1 y n) diferentes, se tiene que

$$\pi(abd)\pi^{-1} = (rst) \in N^{(1)},$$

y esto para todos los 3-ciclos (rst) de S_n.

Finalmente, poniendo $N = G = S_n$ que ciertamente es normal y contiene todos los 3-ciclos de S_n, se tiene que $N^{(1)} = G^{(1)}$ también contiene a todos los 3-ciclos de S_n. De nuevo, por la primera parte de la demostración, como $G^{(1)} \lhd G$ contiene a todos los 3-ciclos, entonces $G^{(2)} \lhd G$ también contiene a todas los 3-ciclos. Por inducción se sigue que $G^{(k)}$ contiene a todos los 3-ciclos de S_n. □

COROLARIO 11.8. *Si $n \geq 5$, el grupo S_n no es soluble.*

Demostración. Por el lema previo, para $G = S_n$, $G^{(k)}$ contiene a todos los 3-ciclos de S_n para toda $k \geq 0$. Por lo tanto $G^{(k)} \neq 1$ para toda $k \geq 0$, y así por (11.5) $G = S_n$ no es soluble. □

Grupos nilpotentes. Dado cualquier grupo G, se definen los subgrupos $Z^i(G)$ de G como sigue: $Z^0(G) = \{1\}$ es el subgrupo trivial, $Z^1(G)$ es el *centro* $Z(G)$ del grupo G, $Z^2(G)$ es el subgrupo de G correspondiente al centro del cociente $G/Z^1(G)$ (por el teorema de correspondencia, 5.12, los subgrupos del cociente $G/Z^1(G)$ están en correspondencia biyectiva con los subgrupos de G que contienen a $Z^1(G)$ y como el centro $Z(G/Z^1(G))$ es un subgrupo normal de $G/Z^1(G)$, entonces el subgrupo $Z^2(G)$ correspondiente es normal en G); así, $Z^1(G) \subseteq Z^2(G)$. Inductivamente, si $Z^i(G)$ ya está definido, sea $Z^{i+1}(G)$ el subgrupo normal de G correspondiente al centro del cociente $G/Z^i(G)$. Se tiene así una cadena de subgrupos

$$(*) \qquad \{1\} = Z^0(G) \subseteq Z^1(G) \subseteq Z^2(G) \subseteq \cdots \subseteq Z^i(G) \subseteq \cdots \subseteq G$$

donde cada $Z^i(G)$ está definido por

$$Z^i(G)/Z^{i-1}(G) = Z(G/Z^{i-1}(G)).$$

La cadena de subgrupos $(*)$ se llama la *serie central superior* de G. Un grupo G se dice que es *nilpotente* si existe un entero $n \geq 0$ tal que $Z^n(G) = G$. El menor entero que satisface lo anterior se llama la *clase* de G.

Ejemplo 9. El grupo trivial $G = \{1\}$ es el único grupo nilpotente de clase cero. Los grupos abelianos no triviales son grupos nilpotentes de clase 1.

LEMA 11.9. *Todo grupo nilpotente es soluble.*

Demostración. Si G es nilpotente de clase n, se tiene una cadena de subgrupos

$$\{1\} = Z^0(G) \subseteq Z^1(G) \subseteq Z^2(G) \subseteq \cdots \subseteq Z^i(G) \subseteq \cdots \subseteq Z^n(G) = G$$

donde cada $Z^i(G)/Z^{i-1}(G) = Z(G/Z^{i-1}(G))$ por lo que $Z^i(G) \lhd Z^{i+1}(G)$ para cada $i \geq 0$, i.e., la cadena anterior es una serie normal cuyos cocientes son centros de un grupo y por lo tanto son abelianos y así G es soluble. □

LEMA 11.10. *Todo grupo nilpotente (no trivial) tiene centro no trivial.*

Demostración. Si G es nilpotente no trivial y si $Z(G) = 1$, entonces $Z^1(G) = 1$ y así

$$Z^2(G) \simeq Z^2(G)/1 = Z^2(G)/Z^1(G) = Z(G/1) = Z(G) = 1$$

y similarmente se prueba que cada $Z^i(G) = 1$, en contradicción con ser G nilpotente. □

El ejemplo siguiente nos dice que hay grupos solubles no nilpotentes:

Ejemplo 10. En el ejemplo 7 mostramos que el grupo S_3 es soluble. Veremos que no es nilpotente. En efecto, por el lema 11.10 todo grupo nilpotente no trivial tiene centro no trivial, pero por 10.2, $Z(S_3) = 1$.

Más ejemplos de grupos nilpotentes nos los da el lema siguiente:

LEMA 11.11. *Todo p-grupo finito es nilpotente.*

Demostración. Por el lema 9.10, si G es un p-grupo finito, G y todos sus subgrupos y cocientes no triviales tienen centros no triviales. Así, si $Z^i(G) \neq G$ para alguna i, entonces $Z(G/Z^i(G)) \neq 1$, por lo que el subgrupo $Z^{i+1}(G)$ correspondiente es diferente de $Z^i(G)$, i.e., $Z^i(G) \subsetneq Z^{i+1}(G)$. Como G es finito, la cadena $1 \subsetneq \cdots \subsetneq Z^i(G) \subsetneq Z^{i+1}(G)$ no puede ser infinita. Se sigue que algún $Z^i(G) = G$ y así G es nilpotente. □

El lema anterior nos da grupos no abelianos que son nilpotentes y el ejemplo 10 nos da grupos solubles no nilpotentes. Se tienen así inclusiones estrictas entre las siguientes clases de grupos:

$$\text{Grupos abelianos} \subsetneq \text{Grupos nilpotentes} \subsetneq \text{Grupos solubles}.$$

Así como los grupos solubles pueden ser caracterizados usando subgrupos conmutadores, se tiene algo análogo para los grupos nilpotentes y para ésto necesitaremos el concepto siguiente, que generaliza la definición de subgrupo conmutador. Si H y K son dos subgrupos de un grupo G, denotemos con $[H, K]$ al subgrupo de G generado por todos los conmutadores de la forma

$$[h, k] = hkh^{-1}k^{-1} \qquad \text{con} \qquad h \in H \quad \text{y} \quad k \in K.$$

Para comenzar notemos que $[H, K] = [K, H]$, lo cual se sigue de observar que si $h \in H$ y $k \in K$, entonces $(hkh^{-1}k^{-1})^{-1} = khk^{-1}h^{-1}$.

LEMA 11.12. (1) *Sean H y K subgrupos de G. Entonces, $[H, K] \subseteq H$ si y sólo si $K \subseteq N_G(H)$.*

(2) *Sean $K \lhd G$ y $K \subseteq H \subseteq G$. Entonces, $[H, G] \subseteq K$ si y sólo si $H/K \subseteq Z(G/K)$.*

(3) *Sea $f : G \to G'$ un homomorfismo suprayectivo. Si $A \subseteq Z(G)$, entonces $f(A) \subseteq Z(G')$.*

Demostración. (1): Si $[H, K] \subseteq H$, entonces para todo $k \in K$ y $h \in H$, $hkh^{-1}k^{-1} \in H$ y así $kh^{-1}k^{-1} \in H$ para todo $k \in K$ y todo $h^{-1} \in H$, por lo que $K \subseteq N_G(H)$.

Recíprocamente, si $K \subseteq N_G(H)$ entonces para todo $k \in K \subseteq N_G(H)$ y todo $h \in H \lhd N_G(H)$ se tiene que $khk^{-1} \in H$ y así $h(kh^{-1}k^{-1}) \in H$, i.e., $[h, k] \in H$, por lo que $[H, K] \subseteq H$.

(2): Si $[H, G] \subseteq K$, entonces para cualquier clase lateral $hK \in H/K$ y cualquier clase $gK \in G/K$ queremos probar que $hKgK = gKhK$, es decir, que $hgK = ghK$,

i.e., que $(gh)(hg)^{-1} \in K$, i.e., que $ghg^{-1}h^{-1} \in K$, pero esto último se sigue de la hipótesis de que $[H, G] \subseteq K$ y del hecho de que $[H, G] = [G, H]$.

Recíprocamente, si $H/K \subseteq Z(G/K)$, entonces $gh)(hg)^{-1} \in K$ para todo $g \in G$ y $h \in H$. Así, $ghg^{-1}h^{-1} \in K$ para todo $g \in G$ y $h \in H$, i.e, $[G, H] \subseteq K$.

(3): Si $f(a) \in f(A)$ y si $h \in G$, como f es suprayectivo existe un $g \in G$ tal que $h = f(g)$. Entonces

$$\begin{aligned} f(a)h = f(a)f(g) &= f(ag) = f(ga) \quad \text{porque } a \in Z(G) \\ &= f(g)f(a) = hf(a) \end{aligned}$$

y así $f(a) \in Z(G')$. □

Usando los subgrupos $[H, K]$ definidos arriba, dado cualquier grupo G definimos los subgrupos siguientes:

$$\begin{aligned} L_1(G) &:= G \\ L_2(G) &:= [L_1(G), G] = [G, G] \\ L_3(G) &:= [L_2(G), G] \\ &\vdots \\ L_{i+1}(G) &:= [L_i(G), G]. \end{aligned}$$

LEMA 11.13. *Sea G cualquier grupo. Entonces, para todo entero $i \geq 1$,*

(1) $L_{i+1}(G) \subseteq L_i(G)$.

(2) $L_i(G)$ *es un subgrupo normal de* G.

Demostración. (1): Inducción sobre i. Como $L_1(G) = G$ y $L_2(G) = [G, G]$, entonces $L_2(G) \subseteq L_1(G)$. Supongamos ahora que $L_i(G) \subseteq L_{i-1}(G)$. Para cualquier generador $hgh^{-1}g^{-1}$ de $L_{i+1}(G) = [L_i(G), G]$, con $h \in L_i(G)$ y $g \in G$, como $L_i(G) \subseteq L_{i-1}(G)$ entonces $h \in L_{i-1}(G)$, por lo que $hgh^{-1}g^{-1} \in [L_{i-1}(G), G] = L_i(G)$ y así $L_{i+1}(G) \subseteq L_i(G)$.

(2): Como, por la parte (1), $[L_i(G), G] = L_{i+1}(G) \subseteq L_i(G)$, el lema 11.12 (1) implica que $G \subseteq N_G(L_i(G))$, i.e., que $N_G(L_i(G)) = G$ y así $L_i(G) \lhd G$. □

El lema anterior nos dice que se tiene una cadena de subgrupos de G:

$$G =: L_1(G) \supseteq L_2(G) \supseteq \cdots \supseteq L_i(G) \supseteq \cdots \supseteq \{1\} = 1$$

a la que se llama la *serie central inferior* de G. El adjetivo *central* proviene del teorema siguiente, que relaciona la serie descendente anterior con la cadena ascendente dada por centros de cocientes de G y con la noción de nilpotencia:

TEOREMA 11.14. *Sea G un grupo. Entonces, $Z^m(G) = G$ si y sólo si $L_{m+1}(G) = 1$. Se sigue que G es nilpotente de clase m si y sólo si $L_{m+1}(G) = 1$ y m es el menor entero que satisface lo anterior.*

Demostración. Supongamos que $Z^m(G) = G$. Probaremos que

$$(*) \qquad L_{i+1}(G) \subseteq Z^{m-i}(G)$$

por inducción sobre i. Cuando $i = 0$ ambos lados de $(*)$ son iguales a G. Supongamos ahora que $L_{i+1}(G) \subseteq Z^{m-i}(G)$. Entonces,

$$L_{i+2}(G) = [L_{i+1}(G), G] \subseteq [Z^{m-i}(G), G] \subseteq Z^{m-i-1}(G)$$

la primera inclusión por hipótesis de inducción y la última porque, por definición de $Z^{m-i}(G)$, se tiene que $Z^{m-i}(G)/Z^{m-i-1}(G) = Z(G/Z^{m-i-1}(G))$ y luego aplicamos el lema 11.12 (2). Esto prueba $(*)$ para $i + 1$. En particular, para $i = m$, de $(*)$ se sigue que $L_{m+1}(G) \subseteq Z^0(G) = 1$ y así $L_{m+1}(G) = 1$.

Recíprocamente, supongamos ahora que $L_{m+1}(G) = 1$. Probaremos ahora $(*)$ en la forma

$$(**) \qquad L_{m+1-i}(G) \subseteq Z^i(G),$$

notando que $(**)$ es la misma inclusión que $(*)$ ya que la suma de los índices es $m+1$. Para comenzar la inducción, en el caso $i = 0$ ambos lados de $(**)$ son iguales a 1. Asumamos ahora que $L_{m+1-i}(G) \subseteq Z^i(G)$. Entonces, para $i + 1$ observemos que como $[L_{m-i}(G), G] \subseteq L_{m+1-i}(G)$ (de hecho, se tiene la igualdad por definición), por el lema 11.12 (2) se sigue que $L_{m-i}(G)/L_{m+1-i}(G) \subseteq Z(G/L_{m+1-i}(G))$ y si ahora consideramos el homomorfismo suprayectivo inducido por la inclusión de la hipótesis de inducción:

$$\rho : G/L_{m+1-i}(G) \to G/Z^i(G)$$

entonces, por 11.12 (3) se sigue que

$$\begin{aligned} L_{m-i}(G)Z^i(G)/Z^i(G) &= \rho(G/L_{m+1-i}(G)) \\ &\subseteq Z(G/Z^i(G)) = Z^{i+1}(G)/Z^i(G), \end{aligned}$$

por lo que $Z^{i+1}(G) \supseteq L_{m-i}(G)Z^i(G) \supseteq L_{m-i}(G)$, como se quería. Así, la inclusión $(**)$ es válida para todo i, y en particular para $i = m$ se tiene que $G = L_1(G) \subseteq Z^m(G)$, por lo que $Z^m(G) = G$. □

Una consecuencia inmediata de esta caracterización de grupos nilpotentes es el resultado siguiente que nos dice que los grupos nilpotentes tienen algunas de las propiedades de los grupos solubles que probamos en 11.6:

COROLARIO 11.15. (1) *Subgrupos de nilpotentes son nilpotentes.*

(2) *Si G es nilpotente y $H \lhd G$, entonces G/H también es nilpotente.*

Demostración. (1): Si G es nilpotente y $H \subseteq G$, por inducción sobre i se muestra que $L_i(H) \subseteq L_i(G)$, por lo que si $L_m(G) = 1$ se tiene que $L_m(H) = 1$ también.

(2): Para el homomorfismo suprayectivo canónico $\rho : G \to G/H$, por inducción sobre i se prueba que $L_i(G/H) \subseteq \rho(L_i(G))$ y por lo tanto, si $L_m(G) = 1$ entonces $L_m(G/H) = 1$ también. □

Note sin embargo que la parte 3 de 11.6 no es válida para grupos nilpotentes, es decir, la clase de grupos nilpotentes no es cerrada bajo extensiones. El mismo ejemplo S_3 nos sirve ya que el subgrupo $A_3 \lhd S_3$ es abeliano y el cociente S_3/A_3 también es abeliano por lo que tanto el subgrupo A_3 como el cociente S_3/A_3 son nilpotentes, pero S_3 no lo es por el ejemplo 10.

Nuestro objetivo ahora es mostrar que los grupos nilpotentes finitos no están muy lejos de los p-grupos finitos y para ésto necesitaremos los dos lemas siguientes, el primero de los cuales es la versión para grupos nilpotentes del ejercicio 5.

LEMA 11.16. *Si G es el producto directo de un número finito de grupos nilpotentes, entonces G también lo es.*

Demostración. Por inducción sobre el número de factores directos es suficiente considerar el caso cuando $G = H \times K$ es el producto directo de dos grupos nilpotentes. Otra inducción, ahora sobre $i \geq 1$, muestra que

$$L_i(G) = L_i(H \times K) = L_i(H) \times L_i(K) \qquad \text{para todo } i \geq 1.$$

Sean m y n las clases de H y K, respectivamente y sea $t = \max\{m, n\}$. Entonces

$$L_t(G) = L_t(H) \times L_t(K) = 1$$

ya que $L_t(H) \subseteq L_m(H) = 1$ y similarmente para K. □

LEMA 11.17. *Sea G un grupo finito y sea P un p-subgrupo de Sylow de G. Entonces, P es el único p-subgrupo de Sylow de su normalizador $N := N_G(P)$ y el normalizador de N es igual a N.*

Demostración. Para la primera afirmación observe que $P \lhd N_G(P)$ y así P es un p-subgrupo de Sylow de $N = N_G(P)$ y como P es normal en N entonces es el único p-subgrupo de Sylow de N. Para la segunda afirmación, como $N \subseteq N_G(N)$, si existiera un elemento $x \in N_G(N) - N$, entonces $x \notin N = N_G(P)$ por lo que $xPx^{-1} \neq P$. Ahora, como $x \in N_G(N)$, entonces $xNx^{-1} = N$ y como $P \subseteq N = N_G(P)$, entonces $xPx^{-1} \subseteq xNx^{-1} = N$ y así $xPx^{-1} \subseteq N$, con xPx^{-1} un p-subgrupo de Sylow de N distinto de P, en contradicción con la primera parte del lema. □

El teorema siguiente resume las distintas caracterizaciones de nilpotencia:

TEOREMA 11.18 (Burnside-Wielandt). *Sea G un grupo finito. Las afirmaciones siguientes son equivalentes:*

(1) *G es nilpotente.*
(2) *Si H es un subgrupo propio de G, entonces $H \subsetneq N_G(H)$.*
(3) *Para cada primo p sólo existe un único p-subgrupo de Sylow de G.*
(4) *G es el producto directo de sus subgrupos de Sylow.*

Demostración. (1) $\Rightarrow$ (2): Escojamos un índice i tal que $L_{i+1}(G) \subseteq H$ pero $L_i(G) \not\subseteq H$ (esto siempre es posible para cualquier cadena de subgrupos de G que comienza en G y termina en 1). Entonces,

$$[L_i(G), H] \subseteq [L_i(G), G] = L_{i+1}(G) \subseteq H,$$

y así, por 11.12 (1), $L_i(G) \subseteq N_G(H)$, y como $L_i(G) \not\subseteq H$, entonces existe algún elemento en $N_G(H)$ que no está en H.

(2) $\Rightarrow$ (3): Sea P cualquier p-subgrupo de Sylow de G y sea $N = N_G(P)$ su normalizador en G. Por el lema anterior N es igual a su normalizador y por la hipótesis (2) se sigue que N no puede ser un subgrupo propio de G, es decir, $G = N = N_G(P)$ y así $P \lhd N_G(P) = G$, i.e., P es normal en G, y como todos los p-subgrupos de Sylow son conjugados se sigue que todos son iguales a P ya que $P \lhd G$ y por lo tanto sólo hay un p-subgrupo de Sylow para cada primo p.

(3) $\Rightarrow$ (4): Sean $p_1, \ldots, p_m$ todos los divisores primos del orden de G y sean G_{p_i} los (únicos) p_i-subgrupos de Sylow correspondientes. El producto directo $G_{p_1} \cdots G_{p_m}$ es un subgrupo de G cuyo orden es igual al de G. Se sigue que este producto directo debe ser igual a G.

(4) $\Rightarrow$ (1): Si G es el producto directo de sus p-subgrupos de Sylow, por los lemas 11.16 y 11.11 se sigue que G es nilpotente. □

Notas. (1) La noción de *solubilidad* de un grupo tiene su origen en los trabajos de Galois [40] y Abel sobre el problema de la solubilidad mediante radicales de ecuaciones polinomiales de grados ≥ 5. En su libro [11], Camille Jordan reúne la mayoría de sus publicaciones en teoría de grupos dando además un enfoque unificado a resultados previos de Galois, Cauchy y otros creadores de la teoría de grupos. Es en este tratado donde Jordan hace explícitas las nociones de homomorfismo e isomorfismo de grupos (de permutaciones), introduce las nociones de *grupo soluble* y de *serie de composición* y demuestra una parte del teorema de Jordan-Hölder, a saber que los índices de los grupos en cualesquiera dos series de composición son iguales. Fue Otto Hölder, en [42] quien introduce la noción abstracta de grupo cociente y prueba que en cualesquiera dos series de composición de un grupo dado, los grupos cociente correspondientes son isomorfos.

(2) El resultado más general sobre grupos solubles es un célebre teorema de Feit y Thompson (célebre porque demostraba una conjetura importante de Burnside y también por la longitud de la demostración: el artículo de más de 250 páginas ocupa todo un número de la revista donde apareció [32]), y su demostración está mucho más allá de los límites de este texto:

Teorema A (Feit-Thompson). *Todo grupo finito de orden impar es soluble.*

Este teorema se puede formular en forma equivalente, como sigue:

Teorema B (Feit-Thompson). *Todo grupo finito, simple y no abeliano tiene orden par.*

En efecto, supongamos que A es verdadero y sea G un grupo finito simple no abeliano. Si $|G|$ fuera impar, por la hipótesis A, el grupo G sería soluble, lo cual es imposible ya que siendo G simple no tiene subgrupos normales propios, por lo que la única serie normal de G es $1 \lhd G$ cuyo cociente es $G/1 \simeq G$ que no es abeliano.

Recíprocamente, supongamos que B es verdadero y sea G un grupo de orden impar. Sea

$$G = G_0 \supseteq G_1 \supseteq G_2 \supseteq \cdots \supseteq G_n = 1$$

una serie de composición de G, con inclusiones estrictas. Entonces, todos los cocientes G_i/G_{i+1} son simples. Si alguno de estos cocientes fuera no abeliano, por la hipótesis B este cociente tendría orden par, lo cual es imposible ya que como $|G|$ es impar, sus subgrupos G_i tienen orden impar (por Lagrange) y así los cocientes G_i/G_{i+1} también son de orden impar.

(3) La solubilidad de los p-grupos la demostró Sylow en [54].

(4) La solubilidad de los grupos de orden $p^r q^s$, para valores pequeños de p, q, r, s, había sido estudiada por Jordan [44], Frobenius [39], Hölder [44] y Burnside [2], donde se preguntaba por lo que sucedía en el caso general. Los casos especiales mencionados, como vimos en este capítulo, sólo requerían conceptos y resultados elementales de la teoría de grupos.

(5) La demostración general del teorema $p^r q^s$ de Burnside, en [26], es de una naturaleza completamente diferente a la de los casos especiales de la nota anterior, en el sentido de que usaba la *teoría de caracteres de grupos*, lo cual, de cierta forma, legitimaba a ésta como una herramienta poderosa para obtener resultados sobre la estructura de los grupos finitos. Fue hasta 1972 cuando Bender [23] obtuvo una demostración *elemental*, i.e., sin usar representaciones de grupos, del teorema de Burnside.

(6) Así como el término *soluble* fue tomado de la teoría de Galois de las ecuaciones polinomiales algebraicas, el término *nilpotente* fue tomado de la teoría de grupos y álgebras de Lie, cuyo objetivo inicial era desarrollar una teoría de Galois de las ecuaciones diferenciales. Dado un grupo de Lie G (digamos, lineal conexo) con álgebra de Lie correspondiente L, se tiene que $Z^m(G) = G$ si y sólo si el álgebra de Lie L consiste de matrices nilpotentes. En su libro [2], Burnside probó que un grupo finito tiene una serie central si y sólo si es producto directo de sus p-subgrupos de Sylow.

(7) Existe una analogía muy sugerente entre la aritmética de los números naturales $\mathbb{N}$ y algunos aspectos de la teoría de grupos finitos. En esta analogía, un divisor n de un número natural m corresponde a un subgrupo normal N de un grupo G, de tal forma que así como m/n es de nuevo un número natural, el cociente G/N es un grupo. En esta línea de ideas, si pensamos a un primo p como un entero > 1 cuyos únicos divisores son 1 y p mismo, el concepto correspondiente es el de un grupo simple, i.e., aquél cuyos únicos subgrupos normales son el 1 y N mismo. Recordemos ahora que el resultado más importante de la aritmética de $\mathbb{N}$ es el teorema de factorización única, a saber, que todo entero $m > 1$ se puede escribir en forma única (salvo el orden de los factores) como un producto de primos $m = p_1^{e_1} \cdots p_s^{e_s}$. Para poder ver el resultado análogo para grupos finitos conviene reformular el teorema anterior de la forma siguiente: consideremos a m como un producto de primos repetidos de acuerdo a su multiplicidad $m = p_1 p_2 \cdots p_r$ y definamos los enteros m_i como sigue: $m_0 = m$, $m_1 = p_2 \cdots p_r$, $m_3 = p_3 \cdots p_s$, ..., $m_{r-1} = p_r$ y $m_r = 1$, de tal forma que

$$m = m_0 \geq m_1 \geq m_2 \geq m_{r-1} \geq m_r = 1 \tag{1}$$

donde cada $m_{i+1} | m_i$ y además cada cociente m_i/m_{i+1} es primo. Note que en esta descripción de m, los primos p_i que ocurren en la factorización de m y sus multiplicidades e_i están unívocamente determinados por m, pero los enteros m_i no lo están, por ejemplo, si $m = 60 = 2^2 \cdot 3 \cdot 5$, podemos escribir

$$60 \geq 30 \geq 15 \geq 5 \geq 1 \qquad \text{y} \qquad 60 \geq 20 \geq 10 \geq 2 \geq 1.$$

Esta formulación del teorema fundamental de la aritmética es la que tiene su análogo en la teoría de grupos finitos en el teorema de Jordan-Hölder, que dice que, para todo grupo finito G existe una cadena de subgrupos

$$G = G_0 \rhd G_1 \rhd G_2 \rhd \cdots \rhd G_{r-1} \rhd G_r = 1 \tag{2}$$

tal que cada G_{i+1} es normal en G_i y los cocientes G_i/G_{i+1} son simples. Más aún, la familia de grupos simples así obtenida depende sólo de G. Ahora, el teorema fundamental de la aritmética nos dice que el entero m se puede recuperar de la cadena (1) tomando los cocientes $p_i = m_i/m_{i+1}$ primos y sus multiplicidades; en este sentido es natural preguntarse cómo se puede recuperar el grupo G de la cadena (2), es decir,

de los cocientes G_i/G_{i+1}, que son grupos simples, y de sus multiplicidades. La pregunta podría plantearse de la manera siguiente: conociendo todos los grupos simples S_i y usando el teorema de Jordan-Hölder, cómo podemos recuperar cualquier grupo finito G dado. Lo primero que debemos hacer es determinar la lista de grupos simples $S_1, \ldots, S_r$ que aparecen como factores de composición simples de G; el segundo paso sería construir el árbol de subgrupos G_i de G tales que $G_i/G_{i+1} \simeq S_i$, para que al final se tenga que $G_0 = G$. La construcción de este árbol comienza fácilmente ya que como $G_r = 1$, escogemos $G_{r-1} = S_r$ para que se tenga que $G_{r-1}/G_r \simeq S_r$. El paso siguiente, una vez determinados G_r y G_{r-1} es encontrar un grupo G_{r-2} sabiendo que debe satisfacer que $G_{r-2}/G_{r-1} \simeq S_{r-1}$, es decir, el grupo G_{r-2} que buscamos debe tener como subgrupo normal a G_{r-1} y como cociente al grupo simple S_{r-1}. Este paso se conoce como el *problema de extensión de Hölder* y se formula en general como sigue: conociendo un (sub)grupo N y un grupo (cociente) Q, se quieren determinar todos los grupos E tales que $N \lhd E$ y $E/N \simeq Q$. A los grupos E que satisfagan lo anterior se les llama *extensiones de N con cociente Q* y se suele usar la notación siguiente

$$N \rightarrowtail E \twoheadrightarrow Q.$$

En general, así como los enteros m_i no son únicos, los grupos E tampoco son únicos; un ejemplo es el siguiente: si $N = \mathbb{Z}/3\mathbb{Z}$ y $Q = \mathbb{Z}/2\mathbb{Z}$, el problema de extensión

$$\mathbb{Z}/3\mathbb{Z} \rightarrowtail E \twoheadrightarrow \mathbb{Z}/2\mathbb{Z}$$

tiene como soluciones a $E = \mathbb{Z}/6\mathbb{Z}$ y $E = S_3$. La pregunta importante ahora es si existe un método sistemático para construir todas las posibles extensiones de un grupo dado N y con cociente dado Q. La respuesta es afirmativa, como demostró O. Schreier en [51] y que ahora forma parte de la *cohomología de grupos*, un tema que no tratamos en este libro. El método desarrollado por Schreier construye todas las tablas de multiplicación posibles para el grupo E, sin embargo hasta la fecha no se conoce un procedimiento general para identificar tablas de multiplicación correspondientes a grupos isomorfos, por lo que la lista de tablas de multiplicación está, en general, plagada de repeticiones. De todas formas, usando el procedimiento de Schreier se puede obtener un grupo G_{i-1} a partir del grupo G_i y con cociente S_i, que satisface que $G_{i-1}/G_i \simeq S_i$.

El método anterior da sentido a la afirmación de que los grupos simples son los ladrillos a partir de los cuales se pueden obtener todos los grupos finitos y es por eso que el teorema de clasificación de los grupos simples finitos tiene una gran importancia.

EJERCICIO 1. Si G es un grupo finito, demuestre que una serie de composición de G es una serie normal de longitud máxima.

EJERCICIO 2. Si $H \lhd G$ y si H y G/H son p-grupos, demuestre que G también es un p-grupo.

EJERCICIO 3. Si G es un p-grupo finito y si $H \subseteq G$ es un subgrupo propio de orden p^k, demuestre que H se puede meter en un subgrupo de G de orden p^{k+1}. Concluya que todo subgrupo máximo de G tiene índice p.

EJERCICIO 4. Demuestre que los grupos diédricos D_{2n} son solubles.

EJERCICIO 5. Si H y K son grupos solubles, demuestre que $G = H \times K$ también es soluble.

EJERCICIO 6. Si G es un grupo finito, soluble y simple, demuestre que G es cíclico de orden primo p.

EJERCICIO 7. Si G es un grupo de orden p^2q, con p, q primos, demuestre que G es producto directo de sus subgrupos de Sylow.

EJERCICIO 8. Si H y K son subgrupos solubles de un grupo G y además $H \lhd G$, demuestre que HK es un subgrupo soluble de G.

EJERCICIO 9. Si G es un grupo finito, demuestre que G es soluble si y sólo si G tiene una serie de composición cuyos cocientes G_i/G_{i+1} son cíclicos de orden primo. *Sugerencia:* para la implicación no trivial, si algún cociente abeliano fuera no simple, entonces tendría un subgrupo no trivial H_i/G_{i+1} y observe que H_i/G_{i+1} y $G_i/H_i \simeq (G_i/G_{i+1})/(H_i/G_{i+1})$ son abelianos, por lo que la serie dada se extiende añadiendo a H_i en el lugar correcto. Continúe el proceso anterior.

EJERCICIO 10. Si un grupo soluble G tiene una serie de composición, demuestre que G es finito.

EJERCICIO 11. Sean G un grupo finito y $H \subseteq G$ un subgrupo. Se dice que H es *subnormal* si existen subgrupos $G_i \subseteq G$, $0 \leq i \leq n$, tales que

$$H = G_0 \lhd G_1 \lhd \cdots \lhd G_n = G.$$

Si H es subnormal, demuestre que los cocientes de cualquier serie de composición de H son una subfamilia de los cocientes de una serie de composición de G.

EJERCICIO 12. Con las mismas hipótesis del ejercicio anterior, si además $H \lhd G$, demuestre que los cocientes de una serie de composición de G son la unión de los cocientes de H y de G/H.

EJERCICIO 13. Demuestre que el grupo diédrico D_{2n} es nilpotente si y sólo si n es una potencia de 2.

EJERCICIO 14. Sea G un grupo nilpotente finito de orden n y suponga que m divide a n. Demuestre que G contiene un subgrupo de orden m.

EJERCICIO 15. Sea G un grupo y denotemos con $\Phi(G)$ a la intersección de todos los subgrupos máximos de G. Demuestre que $\Phi(G) \lhd G$. El grupo $\Phi(G)$ se llama el *subgrupo de Frattini* de G.

EJERCICIO 16. Si G es finito, demuestre que $\Phi(G)$ es nilpotente.

EJERCICIO 17. Un elemento $x \in G$ se dice que es un *no generador* si siempre que el conjunto $Y \cup \{x\}$ genere un subgrupo H de G se tiene que Y ya generaba a H. Demuestre que $\Phi(G)$ es el conjunto de todos los no generadores de G.

EJERCICIO 18. Si G es un grupo, demuestre que $G^{(i)} \subseteq L_i(G)$. Use lo anterior para dar otra demostración de que todo grupo nilpotente es soluble.

EJERCICIO 19. (Wielandt). Demuestre que un grupo finito G es nilpotente si y sólo si todo subgrupo propio máximo de G es normal.

EJERCICIO 20. Si G es un grupo no abeliano de orden p^3, para p un primo, demuestre que su centro es igual a su subgrupo conmutador.

EJERCICIO 21. Use el ejercicio anterior para probar que todo grupo no abeliano de orden p^3 es nilpotente de clase 2.

EJERCICIO 22. Si G es nilpotente, demuestre que todo subgrupo de índice primo es normal.

EJERCICIO 23. Demuestre que un grupo finito no trivial G es nilpotente de clase m si y sólo si $G/Z(G)$ es nilpotente de clase $m-1$.

Capítulo 12

Grupos de matrices

EN CAPÍTULOS PREVIOS hemos visto la importancia de los grupos de permutaciones. Otras familias importantes de grupos son las que provienen del álgebra lineal, en particular son de interés los grupos $\mathrm{GL}(n, K)$ de matrices invertibles con entradas en un campo K, por ejemplo $K = \mathbb{R}$ ó $K = \mathbb{C}$. Sin embargo ninguno de estos grupos es finito y sólo en los ejercicios 3 y 4 del capítulo 2 encontramos al grupo $\mathrm{GL}(2, \mathbb{F}_2)$ y a uno de sus subgrupos, que son grupos de matrices finitos. En este capítulo estudiaremos a los grupos $\mathrm{GL}(n, \mathbb{F}_p)$ de matrices invertibles con entradas en $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ con p un primo, algunos de sus subgrupos y cocientes, para culminar con el teorema 12.9 donde exhibiremos una familia de estos cocientes que son simples. Ahora, como la operación del grupo $\mathrm{GL}(n, \mathbb{F}_p)$ es el producto de matrices y como este producto está dado por sumas de productos de las entradas de las matrices involucradas, donde estas entradas son elementos de $\mathbb{F}_p$, comenzamos recordando cómo se suman y multiplican los elementos de $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ y las propiedades que tienen estas operaciones, análogas a las propiedades de las sumas y productos de $\mathbb{Q}$, $\mathbb{R}$ ó $\mathbb{C}$.

Recordemos que $\mathbb{F}_p$ es el conjunto $\mathbb{Z}/p\mathbb{Z}$ de clases residuales módulo p,

$$\mathbb{F}_p = \{[0], [1], [2], \ldots, [p-1]\}$$

y que ya hemos visto que, con la suma definida usando representantes, el conjunto $(\mathbb{F}_p, +)$ es un grupo abeliano. Si ahora definimos el producto de dos clases residuales $[a], [b] \in \mathbb{F}_p$ mediante $[a][b] := [ab]$, eligiendo representantes $a \in [a], b \in [b]$, en forma análoga a como se hizo para la suma, se prueba que este producto está bien definido, es asociativo, conmutativo, distributivo con respecto a la suma y la clase $[1] \in \mathbb{F}_p$ es neutra para el producto. Más aún, si $[a] \in \mathbb{F}_p$ con $[a] \neq [0]$, entonces $p \nmid a$ y como p es primo entonces $\mathrm{mcd}(p, a) = 1$ por lo que 1 es combinación lineal de a y p, es decir, existen enteros u, v tales que $au + pv = 1$ y reduciendo módulo p esta igualdad se vuelve $[a][u] = [1]$ en $\mathbb{F}_p$, ya que $[p] = [0]$. Hemos así mostrado que si $[a] \neq [0]$, entonces existe $[u] \in \mathbb{F}_p$ tal que $[a][u] = [1]$ y decimos que $[u]$ es un inverso multiplicativo de $[a]$ y por lo tanto todo elemento distinto de cero de $\mathbb{F}_p$ tiene inverso multiplicativo. Así, $\mathbb{F}_p$ junto con la suma y producto definidos arriba es un *campo* y como $|\mathbb{F}_p| = p$, entonces $\mathbb{F}_p$ es un campo con un número finito de elementos. Además de los campos finitos $\mathbb{F}_p$ existen otros campos finitos (cuya cardinalidad necesariamente es de la forma p^n,

para p un primo), sin embargo su construcción ya no es tan sencilla y en este capítulo nos restringiremos a los campos finitos $\mathbb{F}_p$ aún cuando los resultados que probaremos siguen siendo válidos para cualquier campo finito.

Si K es cualquier campo, pongamos $K^* := K - \{0\}$ y observemos que, con el producto del campo K, el conjunto K^* es un grupo multiplicativo abeliano. Cuando K es un campo finito, el grupo finito K^* es cíclico y ésto lo probaremos para $K = \mathbb{F}_p$. Necesitaremos el lema siguiente:

LEMA 12.1. *Sea $f(x) \in K[x]$ un polinomio de grado $n \geq 1$. Entonces, existen a lo más n raíces $\alpha \in K$ de $f(x)$.*

Demostración. La demostración es por inducción sobre $n \geq 1$, el caso $n = 1$ es obvio. Sean $n > 1$, $f(x) = a_n x^n + \cdots + a_1 x + a_0$ y supongamos que $f(\alpha) = 0$, con $\alpha \in K$. Entonces,

$$\begin{aligned} f(x) &= f(x) - f(\alpha) \quad \text{(ya que } f(\alpha) = 0\text{)} \\ &= a_n(x^n - \alpha^n) + \cdots + a_2(x^2 - \alpha^2) + a_1(x - \alpha) + a_0(1 - 1) \\ &= (x - \alpha)(a_n(x^{n-1} + \cdots + \alpha^{n-1}) + \cdots + a_2(x + \alpha) + a_1) \\ &= (x - \alpha)g(x) \end{aligned}$$

con $g(x) \in K[x]$ de grado $n - 1$. Es claro que cualquier raíz de $g(x)$ es raíz de $f(x)$ y si β es una raíz de $f(x)$ con $\beta \neq \alpha$, entonces β debe ser una raíz de $g(x)$ ya que $0 = f(\beta) = (\beta - \alpha)g(\beta)$ y como $\beta - \alpha \neq 0$, esto implica que $g(\beta) = 0$. Ahora, por hipótesis de inducción $g(x)$ tiene a lo más $n - 1$ raíces en K y así a lo más hay $n - 1$ posibilidades para β y por lo tanto $f(x)$ tiene a lo más n raíces. □

TEOREMA 12.2. *Si $\mathbb{F}_p$ es un campo finito, el grupo multiplicativo $\mathbb{F}_p^* = \mathbb{F}_p - \{0\}$ es cíclico.*

Demostración. Como el grupo $\mathbb{F}_p^*$ es abeliano finito, podemos usar los resultados sobre exponentes del capítulo 7. Sea $e = e(\mathbb{F}_p^*)$ el exponente del grupo $\mathbb{F}_p^*$. Entonces, $e \leq \left|\mathbb{F}_p^*\right|$. Ahora, para cada $\alpha \in \mathbb{F}_p^*$ se tiene que $\alpha^e = 1$ por definición de exponente, y así cada $\alpha \in \mathbb{F}_p^*$ es raíz del polinomio $x^e - 1 \in \mathbb{F}_p[x]$. Pero este polinomio tiene a lo más e raíces (su grado) por el lema anterior, y por lo tanto $\left|\mathbb{F}_p^*\right| \leq e$. Se sigue que $e = \left|\mathbb{F}_p^*\right|$ y así $\mathbb{F}_p^*$ es cíclico por el corolario 7.4. □

A un generador del grupo $\mathbb{F}_p^*$ se le llama un *elemento primitivo* del campo $\mathbb{F}_p$ o una *raíz primitiva* módulo p.

El grupo lineal general. Si K es cualquier campo, por ejemplo $K = \mathbb{Q}, \mathbb{R}, \mathbb{C}$ ó $\mathbb{F}_p$, denotemos con $\mathrm{GL}(n, K)$ al conjunto de matrices cuadradas de tamaño $n \times n$ con entradas en K y con determinante distinto de cero. Denotaremos a las matrices mediante

$A = (a_{ij})$ con $a_{ij} \in K$ la entrada en el lugar (i, j). Como el determinante de un producto de matrices es el producto de los determinantes de las matrices dadas, el conjunto $\mathrm{GL}(n, K)$ es un grupo, con el producto de matrices como operación binaria, al que llamaremos el *grupo lineal general*. El neutro de este grupo es la matriz identidad I_n con unos en la diagonal y ceros en las otras entradas. Note que si $n \geq 2$ el grupo $\mathrm{GL}(n, K)$ no es abeliano. En el caso cuando K es un campo finito, por ejemplo $\mathbb{F}_p$, el grupo $\mathrm{GL}(n, \mathbb{F}_p)$ es un grupo finito y nuestro primer objetivo es calcular su orden.

TEOREMA 12.3. *El orden del grupo lineal* $\mathrm{GL}(n, \mathbb{F}_p)$ *es*

$$|\mathrm{GL}(n, \mathbb{F}_p)| = (p^n - 1)(p^n - p) \cdots (p^n - p^{n-1}).$$

Demostración. Por inducción sobre n. Si $n = 1$, $\mathrm{GL}(1, \mathbb{F}_p) = \mathbb{F}_p^* = \mathbb{F}_p - \{0\}$ y así $|\mathrm{GL}(1, \mathbb{F}_p)| = p - 1$. Supongamos que el resultado es válido para $k < n$. Observe que $\mathrm{GL}(n, \mathbb{F}_p) \simeq \mathrm{GL}(V)$ donde V es un $\mathbb{F}_p$-espacio vectorial de dimensión n, $\mathrm{GL}(V)$ denota el grupo de isomorfismos lineales de V en V y donde el isomorfismo $\mathrm{GL}(V) \simeq \mathrm{GL}(n, \mathbb{F}_p)$ está dado eligiendo una base ordenada de V. Observe ahora que se tiene una acción $\mathrm{GL}(n, \mathbb{F}_p) \times V \to V$ definida para $A \in \mathrm{GL}(n, \mathbb{F}_p)$ y $v \in V$ como $A \cdot v := T_A(v)$ donde $T_A : V \to V$ es la transformación lineal asociada a A en una base ordenada $\mathcal{B} = \{v_1, \ldots, v_n\}$ de V. A continuación determinaremos las órbitas y algunos estabilizadores de esta acción:

(1) *Órbitas.* Para comenzar, es claro que si $v = 0$, entonces $\mathrm{orb}(0) = \{0\}$. Ahora, si v y w son vectores no nulos de V, entonces existe una matriz $A \in \mathrm{GL}(n, \mathbb{F}_p)$ tal que $T_A(v) = w$ y por lo tanto, si $v \neq 0$ su órbita es $\mathrm{orb}(v) = V - \{0\}$. Observe que como $V \simeq \mathbb{F}_p^n$, entonces $|V| = p^n$ por lo que si $v \neq 0$ el número de elementos de su órbita es $|\mathrm{orb}_G(v)| = p^n - 1$.

(2) *Estabilizadores.* Para el básico $v_1 \in \mathcal{B} \subseteq V$, por definición su estabilizador es

$$G_{v_1} := \{A \in \mathrm{GL}(n, \mathbb{F}_p) \ : \ T_A(v_1) = v_1\},$$

por lo que una matriz $A \in G_{v_1}$ debe ser de la forma

$$A = \begin{pmatrix} 1 & a_{12} & \cdots & a_{1,n} \\ 0 & a_{22} & \cdots & a_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & a_{n,2} & \cdots & a_{n,n} \end{pmatrix}$$

y poniendo

$$M = \begin{pmatrix} a_{12} & \cdots & a_{1,n} \\ a_{22} & \cdots & a_{2,n} \\ \vdots & \ddots & \vdots \\ a_{n,2} & \cdots & a_{n,n} \end{pmatrix}$$

como $0 \neq \det(A) = \det(M)$, entonces M está en $\mathrm{GL}(n-1, \mathbb{F}_p)$. Se sigue que la matriz $A \in G_{v_1}$ debe ser de la forma

$$A = \begin{pmatrix} 1 & a_{12} \cdots a_{1,n} \\ 0 & M \end{pmatrix}$$

con $M \in \mathrm{GL}(n-1, \mathbb{F}_p)$ y los $a_{12}, \ldots, a_{1,n}$ elementos arbitrarios de $\mathbb{F}_p$. Ahora, como hay p posibilidades para cada uno de estos a_{1j}, $2 \leq j \leq n$, entonces hay p^{n-1} maneras de elegir a los a_{1j} y por lo tanto

$$|G_{v_1}| = |\mathrm{GL}(n-1, \mathbb{F}_p)| p^{n-1} = [(p^{n-1}-1)(p^{n-1}-p) \cdots (p^{n-1}-p^{n-2})] p^{n-1}$$

(la última igualdad por hipótesis de inducción). Finalmente, juntando estos cálculos:

$$\begin{aligned} |\mathrm{GL}(n, \mathbb{F}_p)| &= |\operatorname{orb}_G(v_1)||G_{v_1}| \quad \text{(por el teorema órbita-estabilizador (8.2))} \\ &= (p^n-1)[(p^{n-1}-1)(p^{n-1}-p) \cdots (p^{n-1}-p^{n-2})] p^{n-1} \\ &= (p^n-1)[(p^n-p)(p^n-p^2) \cdots (p^n-p^{n-1})] \end{aligned}$$

que es lo que se quería. □

El grupo lineal especial. El determinante $\det : \mathrm{GL}(n, K) \to K^*$ es un homomorfismo de grupos cuyo núcleo

$$\mathrm{SL}(n, K) := \ker(\det) = \{A \in \mathrm{GL}(n, K) \ : \ \det A = 1\}$$

se llama el *grupo lineal especial* y es un subgrupo normal de $\mathrm{GL}(n, K)$. Es claro que el determinante es suprayectivo y así por el primer teorema de isomorfismo de Noether

$$\mathrm{GL}(n, K)/\mathrm{SL}(n, K) \simeq K^*,$$

por lo que, para el caso cuando $K = \mathbb{F}_p$, del teorema anterior se sigue que:

COROLARIO 12.4. *Para $K = \mathbb{F}_p$, el orden del grupo lineal especial es*

$$|\mathrm{SL}(n, \mathbb{F}_p)| = \frac{(p^n-1)(p^n-p) \cdots (p^n-p^{n-1})}{p-1}.$$

□

El grupo lineal proyectivo. Una *matriz escalar* es una matriz de la forma λI_n, donde I_n es la matriz identidad y $\lambda \in K^*$. Es claro que las matrices escalares conmutan con cualquier otra matriz del mismo tamaño y por lo tanto forman un subgrupo normal de cualquier subgrupo de $\mathrm{GL}(n, K)$ que las contenga. Por ejemplo, si consideramos matrices escalares λI_n en el subgrupo $\mathrm{SL}(n, K)$, se debe tener que $\lambda^n = \det(\lambda I_n) = 1$. Así, el subgrupo Z_0 de matrices escalares de $\mathrm{SL}(n, K)$ está formado por las matrices escalares λI_n tales que $\lambda^n = 1$. Al grupo cociente $\mathrm{SL}(n, K)/Z_0$, se le llama el *grupo lineal proyectivo* y se denota mediante $\mathrm{PSL}(n, K)$. Nuestro siguiente objetivo es calcular el orden del grupo $\mathrm{PSL}(n, \mathbb{F}_p)$.

PROPOSICIÓN 12.5. *Para $K = \mathbb{F}_p$, si Z_0 es el subgrupo de matrices escalares de* $\mathrm{SL}(n, \mathbb{F}_p)$, *entonces* $|Z_0| = d$, *donde* $d = \mathrm{mcd}(n, p-1)$.

Demostración. Por las observaciones anteriores, debemos contar cuántos escalares $\lambda \in \mathbb{F}_p^*$ satisfacen que $\lambda^n = 1$. Sea $d = \mathrm{mcd}(p-1, n)$; como d es combinación lineal de $p-1$ y de n, i.e., $d = (p-1)s + nt$ con $s, t \in \mathbb{Z}$, y como $\lambda^{p-1} = 1 = \lambda^n$, entonces $\lambda^d = 1$. Recíprocamente, si $\lambda^d = 1$, como d divide a n, entonces $\lambda^n = 1$ también. Hemos así mostrado que $\lambda^n = 1$ si y sólo si $\lambda^d = 1$ por lo que basta contar cuántos escalares λ satisfacen que $\lambda^d = 1$. Ahora, por el teorema 12.2, el grupo multiplicativo $\mathbb{F}_p^*$ es cíclico de orden $p-1$. Sea ρ un generador de $\mathbb{F}_p^*$. Observemos ahora que $\lambda^d = 1$ si y sólo si $\lambda \in \langle \rho^{(p-1)/d} \rangle$, el cual es un grupo de orden d por la proposición 3.6, y así hay exactamente d posibilidades para el escalar λ, como se quería. □

COROLARIO 12.6. *Si $K = \mathbb{F}_p$ y $d = \mathrm{mcd}(n, p-1)$, entonces el orden del grupo lineal proyectivo es*

$$|\mathrm{PSL}(n, \mathbb{F}_p)| = \frac{(p^n - 1)(p^n - p) \cdots (p^n - p^{n-1})}{d(p-1)}.$$

Demostración. Se sigue de 12.5 y 12.4. □

Transvecciones y los grupos $\mathrm{PSL}(2, \mathbb{F}_p)$. Si $\lambda \neq 0$ en K y si $i \neq j$, denotemos con $E_{ij}(\lambda)$ a la matriz $n \times n$ que es igual a la matriz identidad I_n excepto en que tiene al escalar λ en la entrada (i, j); a la matriz $E_{ij}(\lambda)$ la llamaremos una *transvección*. Observe que el determinante de cualquier transvección es 1 por lo que las transvecciones están en $\mathrm{SL}(n, K)$, y también, para cualquier matriz A de tamaño $n \times n$ con entradas en K, el producto $E_{ij}(\lambda)A$ es la matriz que se obtiene de A sumando λ veces el renglón j de A a su renglón i. A partir de ahora nos restringiremos a los grupos $\mathrm{GL}(2, \mathbb{F}_p)$, sus subgrupos $\mathrm{SL}(2, \mathbb{F}_p)$ y los cocientes $\mathrm{PSL}(2, \mathbb{F}_p)$, con la intención de probar que estos últimos son simples, para $p > 3$. La proposición siguiente es válida para toda n, aunque nosotros sólo la probaremos para $n = 2$:

PROPOSICIÓN 12.7. *Toda matriz $A \in \mathrm{GL}(2, \mathbb{F}_p)$ se puede escribir de la forma TD, donde T es un producto de transvecciones y D es la matriz diagonal* $\begin{pmatrix} 1 & 0 \\ 0 & \det A \end{pmatrix}$. *En particular, cada matriz de $\mathrm{SL}(2, \mathbb{F}_p)$ es un producto de transvecciones.*

Demostración. Sea $A \in \mathrm{GL}(2, \mathbb{F}_p)$. Si sucediera que la entrada $(1,1)$ de A fuera cero, como A es invertible su entrada $(2,1)$ no puede ser cero. Sumando el segundo renglón de A al primero, i.e., multiplicando $E_{12}(1)A$, obtenemos una matriz B cuya entrada $(1,1)$ no es cero. Note que $\det B = \det A$ ya que $\det E_{12}(1) = 1$. Definamos A_1 como A ó B, dependiendo de que la entrada $(1,1)$ no sea cero, digamos $A_1 = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$

con $a \neq 0$. Sumando $(-c/a)$ veces el primer renglón de A_1 a su segundo renglón, i.e., multiplicando $E_{21}(-c/a)A_1$, se obtiene una matriz de la forma

$$A_2 = \begin{pmatrix} a' & b' \\ 0 & d' \end{pmatrix}$$

con $a' \neq 0$ y además $a'd' = \det A_2 = \det A_1 = \det A$ y por lo tanto $d' \neq 0$. Ahora, sumando $(-b'/d')$ veces el segundo renglón de A_2 a su primer renglón se obtiene la matriz diagonal

$$\Delta = E_{12}(-b'/d')A_2 = \begin{pmatrix} \alpha & 0 \\ 0 & \delta \end{pmatrix}$$

con $\alpha\delta = \det \Delta = \det A$. Finalmente, mediante las operaciones en renglones indicadas abajo, i.e., mediante multiplicaciones a la izquierda por transvecciones, llevamos a la matriz Δ a la forma diagonal D:

$$\Delta = \begin{pmatrix} \alpha & 0 \\ 0 & \delta \end{pmatrix} \sim \begin{pmatrix} \alpha & 0 \\ \alpha & \delta \end{pmatrix} \sim \begin{pmatrix} 1 & e \\ \alpha & \delta \end{pmatrix} \sim \begin{pmatrix} 1 & e \\ 0 & f \end{pmatrix} \sim \begin{pmatrix} 1 & 0 \\ 0 & f \end{pmatrix} = D$$

donde $\det A = \det D = f$. Hemos así mostrado que mediante multiplicaciones a la izquierda por transvecciones, llevamos a la matriz A a la matriz diagonal D, i.e., que $EA = D$, donde E es el producto de las transvecciones requiridas. Por lo tanto, como la inversa de una transvección es una transvección, si $T = E^{-1}$ se tiene que $A = TD$, lo cual prueba la primera afirmación. Para la segunda afirmación, note que si $A \in \mathrm{SL}(2, \mathbb{F}_p)$, como $\det A = 1$, entonces $f = 1$ en la matriz diagonal D, i.e., $D = I_2$ es la matriz identidad. □

El lema siguiente nos dice que las transvecciones juegan un papel análogo para los grupos lineales especiales al que juegan los 3-ciclos para los grupos alternantes:

LEMA 12.8. *Si H es un subgrupo normal de $\mathrm{SL}(2, \mathbb{F}_p)$ y H contiene una transvección $E_{ij}(\lambda)$, entonces $H = \mathrm{SL}(2, \mathbb{F}_p)$.*

Demostración. Por la proposición previa las transvecciones generan a $\mathrm{SL}(2, \mathbb{F}_p)$ y así es suficiente mostrar que H contiene a todas las transvecciones. Ahora, como H contiene una transvección $E_{ij}(\lambda)$ y como $i \neq j$, sus posibilidades son $E_{12}(\lambda)$ ó $E_{21}(\lambda)$. Consideremos el primer caso y supongamos que $E_{12}(\lambda) = \begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix}$ está en H. Como H es normal en $\mathrm{SL}(2, \mathbb{F}_p)$, conjugando $E_{12}(\lambda)$ por cualquier matriz $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ de $\mathrm{SL}(2, \mathbb{F}_p)$ obtenemos otra matriz en H:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} = \begin{pmatrix} 1 - \lambda ac & \lambda a^2 \\ -\lambda c^2 & 1 + \lambda ac \end{pmatrix}$$

y observamos que si $c = 0$ este conjugado es $E_{12}(\lambda a^2)$ y si $a = 0$ este conjugado es $E_{21}(-\lambda c^2)$, y ambas matrices están en H, ya que H es normal. Pongamos

$$\Gamma := \{\gamma \in \mathbb{F}_p \ : \ E_{12}(\gamma) \in H\} \cup \{0\}$$

y notemos que Γ es un subgrupo aditivo del grupo $(\mathbb{F}_p, +)$ ya que $E_{12}(\gamma) + E_{12}(\gamma') = E_{12}(\gamma + \gamma')$ y $-E_{12}(\gamma) = E_{12}(-\gamma)$. También, por lo que probamos antes, Γ contiene a todos los elementos de la forma λa^2. Observe ahora que al menos la mitad de los elementos de $\mathbb{F}_p^*$ son cuadrados ya que la función $\phi : \mathbb{F}_p^* \to \mathbb{F}_p^*$ dada por $\alpha \mapsto \alpha^2$, es un homomorfismo de grupos cuya imagen son los cuadrados perfectos de $\mathbb{F}_p^*$ y cuyo núcleo consiste de todos los $\alpha \in \mathbb{F}_p^*$ tales que $\alpha^2 = 1$, i.e., de todos los $\alpha \in \mathbb{F}_p^*$ que son raíces del polinomio $x^2 - 1$, que tiene a lo más dos raíces por el lema 12.1, y por lo tanto el núcleo de ϕ tiene orden ≤ 2. Por el primer teorema de isomorfismo de Noether la imagen de ϕ tiene orden $\geq |\mathbb{F}_p^*|/2$, es decir, al menos la mitad de los elementos de $\mathbb{F}_p^*$ son cuadrados perfectos. Se sigue que, como Γ contiene al 0 y a todos los elementos de la forma λa^2 con $a^2 \in \mathbb{F}_p^*$, entonces Γ contiene más de la mitad de los elementos de $\mathbb{F}_p$ y así, por el teorema de Lagrange se debe tener que $\Gamma = \mathbb{F}_p$. Por definición de Γ se sigue que H contiene a todas las transvecciones de la forma $E_{12}(\gamma)$. Un argumento similar, ahora usando que H contiene a $E_{21}(-\lambda c^2)$, muestra que H contiene a todas las transvecciones de la forma $E_{21}(\gamma)$. Se sigue que si H contiene una transvección de la forma $E_{12}(\lambda)$, entonces H contiene a todas las transvecciones.

Finalmente, si H contiene una transvección de la forma $E_{21}(\lambda)$, al conjugar por cualquier matriz $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ de $\mathrm{SL}(2, \mathbb{F}_p)$ obtenemos otra matriz en H:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & 0 \\ \lambda & 1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} = \begin{pmatrix} 1 + \lambda bd & -\lambda b^2 \\ \lambda d^2 & 1 - \lambda bd \end{pmatrix}$$

y observamos que si $b = 0$ este conjugado es $E_{21}(\lambda d^2)$ y si $d = 0$ este conjugado es $E_{12}(-\lambda b^2)$, y ambas matrices están en H, ya que H es normal. Procedemos entonces como en el caso anterior. □

El resultado principal es:

TEOREMA 12.9. *Si $p > 3$, los grupos $\mathrm{PSL}(2, \mathbb{F}_p)$ son simples.*

DEMOSTRACIÓN (Dickson). Por 12.6, $|\mathrm{PSL}(2, \mathbb{F}_2)| = 6$ y $|\mathrm{PSL}(2, \mathbb{F}_3)| = 12$, por lo que estos grupos no pueden ser simples por el teorema de Sylow (véanse el ejemplo 3 del capítulo 10 y el ejemplo 3 del capítulo 9, sin tomar en cuenta que el grupo es S_3). Supongamos ahora que $p > 3$. Por el teorema de correspondencia, los subgrupos normales de $\mathrm{PSL}(2, \mathbb{F}_p) = \mathrm{SL}(2, \mathbb{F}_p)/Z_0$ corresponden a subgrupos normales H de $\mathrm{SL}(2, \mathbb{F}_p)$ que contienen a Z_0 y así, para mostrar que $\mathrm{PSL}(2, \mathbb{F}_p)$ es simple basta mostrar que si $H \supsetneq Z_0$, entonces $H = \mathrm{SL}(2, \mathbb{F}_p)$. Para ésto, asumamos por un momento

que H contiene una matriz de la forma

$$(*) \qquad A = \begin{pmatrix} r & 0 \\ s & t \end{pmatrix} \quad \text{con } r \neq \pm 1.$$

Entonces, si $S = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$, como H es normal y $S \in \mathrm{SL}(2, \mathbb{F}_p)$, se tiene que $SAS^{-1} \in H$ y como $A^{-1} \in H$, entonces $SAS^{-1}A^{-1} = \begin{pmatrix} 1 & 0 \\ 1 - t^2 & 1 \end{pmatrix}$ también está en H. Ahora, como $\det A = 1$ y como $r \neq \pm 1$, entonces $t \neq \pm 1$ y así $1 - t^2 \neq 0$. Se sigue que $SAS^{-1}A^{-1} = E_{21}(1 - t^2)$ es una transvección en H y así, por el lema anterior, se debe tener que $H = \mathrm{SL}(2, \mathbb{F}_p)$ como se quería. Para terminar la demostración sólo falta probar (*). Ahora, como $H \supsetneq Z_0$, sea $M \in H$ una matriz que no está en Z_0 (i.e., que no es de la forma $M = \lambda I_2$ con $\lambda^2 = 1$ por definición de Z_0). Entonces, M es conjugada, por una matriz de $\mathrm{GL}(2, \mathbb{F}_p)$, a su forma canónica racional que tiene las dos posibilidades siguientes (ya que las únicas formas canónicas racionales posibles para una matriz 2×2 son: la suma directa de dos matrices compañeras 1×1, i.e., una matriz diagonal, o una matriz compañera 2×2):

$$(**) \qquad \begin{pmatrix} r & 0 \\ 0 & t \end{pmatrix} \quad \text{ó} \quad \begin{pmatrix} 0 & a \\ 1 & b \end{pmatrix}$$

y como $\det M = 1$, entonces $a = -1$. Antes de considerar estos dos casos, observemos que si la matriz $M \in H$ es conjugada, por un elemento de $\mathrm{GL}(2, \mathbb{F}_p)$, a una matriz $R = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, entonces existe un escalar $\mu \in \mathbb{F}_p^*$ tal que H contiene a la matriz $\begin{pmatrix} a & \mu^{-1}b \\ \mu c & b \end{pmatrix}$. Para probar ésto, escribamos $M = LRL^{-1}$ con $L \in \mathrm{GL}(2, \mathbb{F}_p)$; por 12.7, $L = TD$ con T un producto de transposiciones y $D = \begin{pmatrix} 1 & 0 \\ 0 & \mu \end{pmatrix}$ con $\mu = \det L$. Se sigue que

$$M = (TD)R(TD)^{-1} = T(DRD^{-1})T^{-1} = T \begin{pmatrix} 1 & 0 \\ 0 & \mu \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & \mu^{-1} \end{pmatrix} T^{-1}$$

$$= T \begin{pmatrix} a & \mu^{-1}b \\ \mu c & d \end{pmatrix} T^{-1},$$

con T un producto de transposiciones por lo que $T \in \mathrm{SL}(2, \mathbb{F}_p)$. Se sigue que H contiene a la matriz $B = \begin{pmatrix} a & \mu^{-1}b \\ \mu c & c \end{pmatrix}$ como se quería. Regresemos ahora a los dos casos (**) de la forma canónica racional asociada a M: en el primer caso ya tenemos a la matriz deseada, porque la matriz $B \in H$ es $B = \begin{pmatrix} r & 0 \\ 0 & t \end{pmatrix}$ y además la igualdad

$r = \pm 1$ implicaría que $t = \pm 1$ y por lo tanto $M = \begin{pmatrix} r & 0 \\ 0 & t \end{pmatrix} = \begin{pmatrix} \pm 1 & 0 \\ 0 & \pm 1 \end{pmatrix} = \pm I_2$ estaría en Z_0, una contradicción, y así $r \neq \pm 1$. En el segundo caso (donde $a = -1$), la matriz $B \in H$ es $B = \begin{pmatrix} 0 & -\mu^{-1} \\ \mu & b \end{pmatrix}$, por lo que si $U = \begin{pmatrix} \gamma^{-1} & 0 \\ 0 & \gamma \end{pmatrix}$ con cualquier $\gamma \in \mathbb{F}_p^*$, entonces $U \in \mathrm{SL}(2, \mathbb{F}_p)$ y así $UBU^{-1} \in H$ y como $B^{-1} \in H$, entonces $UBU^{-1}B^{-1}$ está en H, i.e. la matriz

$$C = UBU^{-1}B^{-1} = \begin{pmatrix} \gamma^{-2} & 0 \\ \mu b(\gamma^2 - 1) & \gamma^2 \end{pmatrix}$$

está en H. Notamos ahora que, si $\gamma^{-2} \neq \pm 1$, i.e., si $\gamma^4 \neq 1$, entonces ya terminamos de probar $(*)$. Observamos ahora que éste es el caso si $p > 5$ porque tal $\gamma \in \mathbb{F}_p^*$ existe ya que el polinomio $x^4 - 1$ tiene a lo más cuatro raíces en $\mathbb{F}_p$ por 12.1. Si $p = 5$, hay dos posibilidades, la primera es cuando la entrada b de B no es cero; en este caso escogemos un $\gamma \in \mathbb{F}_5 \simeq \mathbb{Z}/5\mathbb{Z}$ tal que $\gamma^2 - 1 \neq 0$. Listando las posibilidades para γ en $\mathbb{F}_5$ notamos que se debe tener que $\gamma^2 = -1$. Entonces, la entrada $(2,1)$ de C, $\lambda := \mu b(\gamma^2 - 1)$, no es cero y como $\gamma^2 = -1$, la matriz C es de la forma $C = \begin{pmatrix} -1 & 0 \\ \lambda & -1 \end{pmatrix}$, y como $C \in H$ entonces H contiene a la matriz $C^2 = \begin{pmatrix} 1 & 0 \\ -2\lambda & 1 \end{pmatrix} = E_{21}(-2\lambda)$, i.e., H contiene una transvección y por lo tanto $H = \mathrm{SL}(2, \mathbb{F}_p)$ por el lema 12.8. La segunda posibilidad es cuando la entrada $b = 0$; en este caso B es de la forma $B = \begin{pmatrix} 0 & -\mu^{-1} \\ \mu & 0 \end{pmatrix} \in H$, por lo que H contiene a la matriz

$$\begin{pmatrix} 1 & \gamma \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & -\mu^{-1} \\ \mu & 0 \end{pmatrix} \begin{pmatrix} 1 & -\gamma \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} \mu\gamma & -\mu\gamma^2 - \mu^{-1} \\ * & * \end{pmatrix}$$

de tal forma que escogiendo $\gamma = 2\mu^{-1}$ se tiene que el renglón superior de esta matriz es de la forma $[2, 0]$ como se quería (ya que $-\mu\gamma^2 - \mu^{-1} = -5\mu^{-1} = 0$ en $\mathbb{F}_5$). □

Notas. El teorema anterior nos da una familia infinita de grupos simples. Note sin embargo que $|\mathrm{PSL}(2, \mathbb{F}_5)| = 60$, que es igual al orden de A_5. En el ejercicio 1 se pide probar que cualesquiera dos grupos simples de orden 60 son isomorfos. En [22], E. Artin muestra que sólo hay 5 miembros de la familia $\mathrm{PSL}(2, \mathbb{F}_p)$ que son miembros de otras familias de grupos simples. Con un argumento esencialmente geométrico, ver, por ejemplo [16], se puede probar que los grupos $\mathrm{PSL}(n, K)$ son simples para toda $n > 2$ y cualquier campo K.

EJERCICIO 1. Demuestre que cualesquiera dos grupos simples de orden 60 son isomorfos.

EJERCICIO 2. Demuestre que, si $p > 3$ el subgrupo conmutador de $\mathrm{GL}(2, \mathbb{F}_p)$ es $\mathrm{SL}(2, \mathbb{F}_p)$.

EJERCICIO 3. Calcule los subgrupos conmutadores de $\mathrm{GL}(2, \mathbb{F}_2)$ y $\mathrm{GL}(2, \mathbb{F}_3)$.

EJERCICIO 4. Exhiba un 2-subgrupo de Sylow de $\mathrm{SL}(2, \mathbb{F}_3)$.

EJERCICIO 5. Muestre que $\mathrm{PSL}(2, \mathbb{F}_2) \simeq S_3$.

EJERCICIO 6. Muestre que $\mathrm{PSL}(2, \mathbb{F}_3) \simeq A_4$.

EJERCICIO 7. Demuestre que el centro del grupo $\mathrm{SL}(n, K)$ es el grupo Z_0 de matrices escalares λI_n que satisfacen que $\lambda^n = 1$. *Sugerencia*: para la inclusión no trivial, suponga que A está en el centro y vea a A como una transformación lineal de K^n en sí mismo y con la base canónica. Para la transvección $E = E_{st}(1)$ calcule su acción en los básicos de K^n y luego calcule la acción de AE y EA en estos básicos para concluir que A es diagonal. Finalmente pruebe que los elementos de la diagonal son todos iguales.

Capítulo 13

Representaciones lineales de grupos finitos

En matemáticas, como en otros ámbitos, la *hibridación* enriquece las estructuras. En este libro hemos estudiado la estructura de grupo y hemos visto ejemplos que aparecen naturalmente en varias ramas de la matemática. Uno de estos ejemplos, y el más importante por razones varias, es el de los grupos de matrices $\mathrm{GL}(n, K)$ cuyo origen está en el estudio de los *operadores lineales invertibles* en un K-espacio vectorial V de dimensión finita. Recordemos cómo se definen estos grupos: dado un K-espacio vectorial V, de dimensión finita n, denotemos con $\mathrm{GL}(V)$ al conjunto de operadores lineales $T : V \to V$ invertibles, i.e., tales que T tiene inverso $T^{-1} : V \to V$ que también es lineal; el conjunto $\mathrm{GL}(V)$, con la composición de funciones como operación binaria, es un grupo. Eligiendo una base $\mathcal{B} = \{v_1, \ldots, v_n\}$ de V se asocia a cualquier operador lineal $T \in \mathrm{GL}(V)$ una matriz $[T]_{\mathcal{B}}$ de tamaño $n \times n$ cuyas entradas a_{ij} se obtienen expresando las imágenes $T(v_j)$ de los vectores básicos v_j en términos de la base $\mathcal{B}$:

$$Tv_j = \sum_i a_{ij} v_i.$$

El hecho de que T sea invertible es equivalente a que el determinante de la matriz $[T]_{\mathcal{B}}$ sea $\neq 0$, es decir, a que $[T]_{\mathcal{B}} \in \mathrm{GL}(n, K)$. Es fácil probar, véase el ejercicio 1, que la correspondencia anterior es un isomorfismo de grupos

$$\mathrm{GL}(V) \simeq \mathrm{GL}(n, K)$$

que identifica a los operadores lineales invertibles con las matrices cuadradas cuyo determinante no es nulo. Así, dada una matriz $A \in \mathrm{GL}(n, K)$ denotamos con $T_A : V \to V$ al operador lineal invertible correspondiente. Usando esta correspondencia podemos definir una función

$$(\dagger) \qquad \mathrm{GL}(n, K) \times V \to V$$

mediante $(A, v) \mapsto A \cdot v := T_A(v)$, que claramente satisface las propiedades:

(i) $I_n \cdot v = T_{I_n}(v) = \mathrm{id}_V(v) = v$.

(ii) $(AB) \cdot v = T_{AB}(v) = T_A \circ T_B(v) = T_A(T_B v) = T_A(B \cdot v) = A \cdot (B \cdot v)$

y por lo tanto la función (†) define una *acción* de $\mathrm{GL}(n, K)$ en V. Ahora, recordando que, como espacio vectorial, V tiene las operaciones de suma de vectores y de producto de un escalar por un vector, observamos que estas operaciones son *compatibles* con la acción (†) anterior, es decir, se satisface que:

(iii) $A \cdot (v + w) = T_A(v + w) = T_A(v) + T_A(w) = A \cdot v + A \cdot w$

y

(iv) $A(\lambda v) = T_A(\lambda v) = \lambda T_A(v) = \lambda \cdot (A \cdot v)$.

Para recordar que las propiedades (iii) y (iv) provienen del hecho de que T_A es lineal, diremos que la acción (†) es una *acción lineal.*

Acciones lineales. Supongamos ahora que G es cualquier grupo y que se tiene una acción de G en un K-espacio vectorial V, de dimensión finita, es decir, una función

$$* : G \times V \to V$$

que satisface los axiomas:

(i) $e * v = v$, para todo $v \in V$ y donde e es el neutro de G.

(ii) $(\sigma\tau) * v = \sigma * (\tau * v)$, para todo $\sigma, \tau \in G$ y $v \in V$.

y que además es *compatible* con las operaciones del espacio vectorial V, es decir,

(iii) $\sigma * (v + w) = \sigma * v + \sigma * w$, para $\sigma \in G$ y $v, w \in V$.

(iv) $\sigma * (\lambda v) = \lambda(\sigma * v)$, para $\lambda \in K$, $v \in V$ y $\sigma \in G$.

Cuando esto suceda, diremos que la acción es *G-lineal* y que V es un *G-espacio vectorial.*

Recordando ahora que en los ejercicios 1 y 2 del capítulo 8 se mostró que las acciones de un grupo G en un conjunto Y están en correspondencia biyectiva con los homomorfismos del grupo G en el grupo simétrico S_Y de Y, es natural que nos preguntemos por lo que sucede cuando se tienen acciones lineales de un grupo G en un K-espacio vectorial V. Para ver lo que sucede en este caso, supongamos primero que se tiene una acción lineal

$$* : G \times V \to V$$

y usando esta acción definamos la función

$$\rho : G \to \mathrm{GL}(V)$$

como sigue: para $\sigma \in G$, $\rho(\sigma) \in \mathrm{GL}(V)$ es el operador lineal $\rho(\sigma) : V \to V$ dado por

$$\rho(\sigma)(v) := \sigma * v.$$

Note que, como en los ejercicios mencionados del capítulo 8, se tiene que $\rho(\sigma) : V \to V$ es, en efecto, biyectiva, y es fácil ver que es lineal. Observemos ahora que la función

$\rho : G \to \mathrm{GL}(V)$ es un homomorfismo de grupos ya que si $\sigma, \tau \in G$, entonces para todo $v \in V$:

$$\rho(\sigma\tau)v = (\sigma\tau) * v = \sigma * (\tau * v) = \sigma * (\rho(\tau)v) = \rho(\sigma)(\rho(\tau)v) = (\rho(\sigma) \circ \rho(\tau))v$$

por lo que $\rho(\sigma\tau) = \rho(\sigma) \circ \rho(\tau)$.

Recíprocamente, supongamos ahora que se tiene un homomorfismo de grupos

$$\rho : G \to \mathrm{GL}(V)$$

y definamos la función

$$* : G \times V \to V$$

mediante $\sigma * v := \rho(\sigma)(v)$. La función $*$ es una acción lineal ya que:

(i) Si $\sigma = e$ es el neutro de G, entonces

$$e * v := \rho(e)(v) = \mathrm{id}_V(v) = v$$

para todo $v \in V$.

(ii) Si $\sigma, \tau \in G$ y $v \in V$, entonces

$$(\sigma\tau) * v := \rho(\sigma\tau)(v) = \rho(\sigma) \circ \rho(\tau)v = \rho(\sigma)(\rho(\tau)v) = \rho(\sigma)(\tau * v) = \sigma * (\tau * v).$$

y además es lineal, es decir,

(iii) Para $\sigma \in G$ y $v, w \in V$,

$$\sigma * (v + w) = \rho(\sigma)(v + w) = \rho(\sigma)v + \rho(\sigma)w = \sigma * v + \sigma * w.$$

(iv) Para $\lambda \in K$, $v \in V$ y $\sigma \in G$,

$$\sigma * (\lambda v) = \rho(\sigma)(\lambda v) = \lambda(\rho(\sigma)v) = \lambda(\sigma * v).$$

Dejamos como un ejercicio el probar que las correspondencias anteriores son inversas una de la otra. Con ésto se ha probado:

TEOREMA 13.1. *Existe una correspondencia biyectiva entre el conjunto de acciones lineales de un grupo G en un K-espacio vectorial V y el conjunto de homomorfismos de G en* $\mathrm{GL}(V)$.

□

Representaciones lineales. Si G es un grupo y V es un K-espacio vectorial, una *representación lineal* de G en V es un homomorfismo

$$\rho : G \to \mathrm{GL}(V).$$

El teorema anterior nos dice que estudiar las representaciones lineales de un grupo G en un espacio vectorial V, es equivalente a estudiar las acciones lineales de G en V.

En adelante, nos restringiremos a estudiar representaciones de *grupos finitos* en espacios vectoriales *complejos* y de dimensión finita. A la dimensión del $\mathbb{C}$-espacio vectorial V la llamaremos el *grado* de la representación $\rho : G \to \mathrm{GL}(V)$ y a V lo llamaremos el *espacio de la representación*; algunas veces también diremos que V es la representación de G.

La definición anterior se puede poner en términos de matrices si damos una base $\mathcal{B} = \{v_1, \ldots, v_n\}$ de V, de tal forma que el isomorfismo $\mathrm{GL}(V) \simeq \mathrm{GL}(n, \mathbb{C})$ (es importante enfatizar que éste depende de la base) compuesto con la representación $\rho : G \to \mathrm{GL}(V)$ nos da un homomorfismo de grupos, al cual seguiremos denotando por ρ,

$$\rho : G \to \mathrm{GL}(n, \mathbb{C})$$

que asocia a cada elemento $\sigma \in G$ del grupo (abstracto) una matriz (concreta) invertible $\rho(\sigma) \in \mathrm{GL}(n, \mathbb{C})$

Para comenzar a estudiar las representaciones de un grupo finito, conviene ponernos de acuerdo en cuándo dos de ellas son la *misma*. Dadas dos representaciones de un grupo G

$$\rho : G \to \mathrm{GL}(V) \qquad \text{y} \qquad \rho' : G \to \mathrm{GL}(V')$$

diremos que son *equivalentes* o *isomorfas*, si existe un isomorfismo lineal $f : V \to V'$ tal que para todo $s \in G$ se tiene que

$$f \circ \rho(s) = \rho'(s) \circ f$$

para todo $s \in G$, es decir, si los diagramas siguientes conmutan

$$\begin{array}{ccc} V & \xrightarrow{f} & V' \\ {\scriptstyle \rho(s)}\downarrow & & \downarrow{\scriptstyle \rho'(s)} \\ V & \xrightarrow[f]{} & V' \end{array}$$

Note que como los espacios V y V' son isomorfos, los grados de representaciones equivalentes son iguales.

Ejemplo 1. Si G es un grupo finito de orden n, una representación de grado 1 de G es un homomorfismo $\rho : G \to \mathbb{C}^*$, ya que $\mathrm{GL}(1, \mathbb{C}) = \mathbb{C}^*$. Como $|G| = n$, entonces todo $g \in G$ satisface que $g^n = 1$ y como ρ es un homomorfismo, entonces $1 = \rho(g^n) = \rho(g)^n$ y por lo tanto el complejo $\rho(g) \in \mathbb{C}^*$ es una raíz n-ésima de la unidad. En particular, su módulo es $|\rho(g)| = 1$.

Ejemplo 2. Si G es un grupo finito y se define $\rho : G \to \mathbb{C}^*$ mediante $\rho(g) := 1$ para todo $g \in G$, ésta es una representación de grado 1 a la que se llama la *representación trivial o principal* de G.

Ejemplo 3. Si $G = \mathbb{Z}/n\mathbb{Z}$ y si $\rho : \mathbb{Z}/n\mathbb{Z} \to \mathbb{C}^*$ es una representación de grado 1, por el ejemplo 1 la imagen de ρ está contenida en el grupo $\mu_n \subseteq \mathbb{C}^*$ de raíces n-ésimas de la unidad. Ahora, como $\mathbb{Z}/n\mathbb{Z}$ es cíclico, la representación ρ está determinada por su valor en un generador de $\mathbb{Z}/n\mathbb{Z}$. Sea $1 \in \mathbb{Z}/n\mathbb{Z}$ el generador canónico; entonces para cada raíz $\omega \in \mu_n$ podemos definir $\rho_\omega : \mathbb{Z}/n\mathbb{Z} \to \mathbb{C}^*$ mediante $\rho_\omega(1) := \omega$ (y para $k \in \mathbb{Z}/n\mathbb{Z}$, $\rho_\omega(k) := \omega^k$, $0 \leq k < n$.

Ejemplo 4. Si S_n es el grupo simétrico, la *función signo* $\operatorname{sgn} : S_n \to \{+1, -1\} \subseteq \mathbb{C}^*$ es una representación de grado 1.

Ejemplo 5. (*La representación regular*). Sea G cualquier grupo finito de orden n y sea V el $\mathbb{C}$-espacio vectorial de dimensión n con base $\mathcal{B} = \{v_g\}_{g \in G}$ indexada por los elementos del grupo. Para cada $\sigma \in G$ definamos la función $\rho(\sigma) : \mathcal{B} \to \mathcal{B}$ mediante $\rho(\sigma)(v_g) = v_{\sigma g}$ y notemos que $\rho(\sigma)$ es una biyección. Entonces, la función $\rho(\sigma)$ se extiende linealmente a un isomorfismo de espacios vectoriales $\rho(\sigma) : V \to V$. Mostraremos que la función

$$\rho : G \to \mathrm{GL}(V) \qquad \text{dada por} \qquad \sigma \mapsto \rho(\sigma)$$

es un homomorfismo. En efecto, si $\sigma, \tau \in G$ y si $v_g \in \mathcal{B}$, entonces

$$\rho(\sigma\tau)v_g = v_{(\sigma\tau)g} = v_{\sigma(\tau g)} = \rho(\sigma)v_{\tau g} = \rho(\sigma)(\rho(\tau)v_g) = \rho(\sigma)\rho(\tau)v_g$$

y así $\rho(\sigma\tau) = \rho(\sigma)\rho(\tau)$. La representación $\rho : G \to \mathrm{GL}(V)$ anterior se llama la *representación regular* de G y, por definición, su grado es el orden de G. Note que, si $g \in G$, entonces $\rho(g)v_1 = v_g$ por lo que las imágenes de v_1 forman una base de V.

Observación. Si ρ es la representación regular, la matriz asociada a cada $\rho(\sigma)$ consiste de ceros y unos (ejercicio 2), lo cual puede observarse en el ejemplo siguiente:

Ejemplo 6. (Subejemplo del ejemplo anterior). Sea $G = S_3$ el grupo simétrico en 3 letras, digamos

$$S_3 = \{1,\ (1\ 2),\ (1\ 3),\ (2\ 3),\ (1\ 2\ 3),\ (1\ 3\ 2)\}.$$

Entonces, $|S_3| = 6$ y la representación regular de S_3, $\rho : S_3 \to \mathrm{GL}(6, \mathbb{C})$ estará determinada una vez que conozcamos sus valores en los generadores (1 2) y (1 2 3) de S_3, (ver 4.15). Sean v_1, $v_{(12)}$, $v_{(13)}$, $v_{(23)}$, $v_{(123)}$ y $v_{(132)}$ una base del espacio V. Para calcular la matriz asociada a $\rho(12) : V \to V$ debemos calcular su valor en cada elemento de la base y luego expresarlo como combinación lineal de los vectores de la misma base:

$$\begin{aligned}
\rho(12)v_1 = v_{(12)1} = v_{(12)} &= 0v_1+1v_{(12)}+0v_{(13)}+0v_{(23)}+0v_{(123)}+0v_{(132)}\\
\rho(12)v_{(12)} = v_{(12)(12)} = v_1 &= 1v_1+0v_{(12)}+0v_{(13)}+0v_{(23)}+0v_{(123)}+0v_{(132)}\\
\rho(12)v_{(13)} = v_{(12)(13)} = v_{(132)} &= 0v_1+0v_{(12)}+0v_{(13)}+0v_{(23)}+0v_{(123)}+1v_{(132)}\\
\rho(12)v_{(23)} = v_{(12)(23)} = v_{(123)} &= 0v_1+0v_{(12)}+0v_{(13)}+0v_{(23)}+1v_{(123)}+0v_{(132)}\\
\rho(12)v_{(123)} = v_{(12)(123)} = v_{(23)} &= 0v_1+0v_{(12)}+0v_{(13)}+1v_{(23)}+0v_{(123)}+0v_{(132)}\\
\rho(12)v_{(132)} = v_{(12)(132)} = v_{(13)} &= 0v_1+0v_{(12)}+1v_{(13)}+0v_{(23)}+0v_{(123)}+0v_{(132)}
\end{aligned}$$

y así la matriz asociada a $\rho(12)$ es la transpuesta de la matriz de coeficientes anterior:

$$\rho(12) = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \end{pmatrix}$$

En forma similar se calcula

$$\rho(123) = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}.$$

Ejemplo 7. Al definir la representación regular de un grupo finito G, tomamos una base $\mathcal{B} = \{v_g\}_{g\in G}$ indexada por los elementos de G y consideramos la acción natural de G en $\mathcal{B}$, $G \times \mathcal{B} \to \mathcal{B}$ dada por $\sigma * v_g := v_{\sigma g}$. En general, si Y es un G-conjunto finito con acción $G \times Y \to Y$, consideremos el espacio vectorial V con base $\mathcal{B} = \{v_x\}_{x\in Y}$ indexada por los elementos de Y. La acción de G en Y induce una acción de G en $\mathcal{B}$ mediante $\sigma * v_x := v_{\sigma * x}$ y esta acción corresponde a un homomorfismo $\phi : G \to S_{\mathcal{B}}$ donde $\phi(\sigma) : \mathcal{B} \to \mathcal{B}$ es la función $\phi(\sigma)(v_x) := \sigma * v_x = v_{\sigma * x}$. Como $\phi(\sigma)$ es biyectiva, se extiende por linealidad a un isomorfismo de espacios vectoriales $\phi(\sigma) : V \to V$. La función $\phi : G \to \mathrm{GL}(V)$ así definida es una representación de G en V de grado $n = |Y|$, a la que se llama la *representación por permutaciones* del grupo G.

Un caso particular es cuando $Y = \mathbb{I}_n$ y $G = S_n$, obteniendo así la representación

$$\rho : S_n \to \mathrm{GL}(n, \mathbb{C})$$

del grupo simétrico S_n. Esta representación identifica una permutación $\sigma \in S_n$ con una matriz $\rho(\sigma) \in \mathrm{GL}(n, \mathbb{C})$ escogiendo como $V = \mathbb{C}^n$ con base la canónica $\{e_1, \ldots, e_n\}$ (indexada por los enteros $1, 2, \ldots, n \in \mathbb{I}_n$).

Subrepresentaciones. Si $\rho : G \to \mathrm{GL}(V)$ es una representación de grado $n < \infty$, y $W \subseteq V$ es un subespacio vectorial, diremos que W es *estable* o *invariante* bajo G si para cualesquiera $\sigma \in G$ y $w \in W$ se tiene que $\rho(\sigma)w \in W$. Si W es estable bajo G, para cada $\sigma \in G$ la restricción $\rho(\sigma)|_W$ es un isomorfismo de W en sí mismo (ya que es inyectivo y W es de dimensión finita). Se sigue que la restricción de ρ a W es una representación de G en W, $\rho_W : G \to \mathrm{GL}(W)$, y se dice que ρ_W es una *subrepresentación* de ρ.

Ejemplo 8. Los subespacios $\{0\}$ y V de V son G-invariantes.

Ejemplo 9. Sea $\rho : G \to \mathrm{GL}(V)$ la representación regular de G y supongamos que V tiene como base a $\mathcal{B} = \{v_g\}_{g \in G}$. Consideremos el vector $v := \sum_{g \in G} v_g$ y el subespacio $W = \langle v \rangle$ generado por v. Por la independencia lineal de $\mathcal{B}$, el vector $v \neq 0$, por lo que $\dim_{\mathbb{C}} W = 1$. Ahora, como la acción de G en $\mathcal{B}$ sólo permuta los vectores de la base, entonces para cualquier $\sigma \in G$

$$\rho(\sigma)v = \rho(\sigma)\Big(\sum_{g \in G} v_g\Big) = \sum_{g \in G} \rho(\sigma)v_g = \sum_{g \in G} v_{\sigma g} = v$$

y por lo tanto W es invariante bajo G. Así $\rho_W : G \to \mathrm{GL}(W)$ es una subrepresentación de ρ de grado 1. Note que como $\{v\}$ es base de W y como $\rho(\sigma)v = v$, para todo $\sigma \in G$, entonces la representación matricial $\rho_W : G \to \mathrm{GL}(1, \mathbb{C}) = \mathbb{C}^*$ está dada por $\rho(\sigma) = 1$, para todo $\sigma \in G$, i.e., ρ_W es la representación trivial de G.

Ejemplo 10. De nuevo, sea $\rho : G \to \mathrm{GL}(V)$ la representación regular de G y sea $\mathcal{B} = \{v_g\}_{g \in G}$ una base de V. Considere ahora el subespacio W' generado por los v_g con $g \neq 1$ en G y observe que W' *no es estable* porque si $g \neq 1$, entonces $v_g \in W'$ pero $\rho(g^{-1})v_g = v_{g^{-1}g} = v_1 \notin W'$.

Note que $V = W + W'$ y que $W \cap W' = 0$ por lo que $V = W \oplus W'$, con W como en el ejemplo 9. Así, V es suma directa de un subespacio G-invariante y uno que no lo es. La pregunta natural es: ¿será V la suma de dos subespacios G-invariantes?

TEOREMA 13.2. *Sean G un grupo finito y $\rho : G \to \mathrm{GL}(V)$ una representación de G de grado $n < \infty$. Si $W \subseteq V$ es un subespacio G-invariante, entonces existe un subespacio G-invariante $W^0 \subseteq V$ tal que $V = W \oplus W^0$.*

Demostración. Como $W \subseteq V$, entonces existe un complemento directo $W' \subseteq V$ tal que $V = W \oplus W'$. Sea $p : V \to W$ la proyección en el primer sumando directo.

Entonces, $\ker p = W'$ e $\operatorname{Im} p = W$. Consideremos la transformación lineal

$$p^0 := \frac{1}{|G|} \sum_{g \in G} \rho(g) \circ p \circ \rho(g^{-1}) : V \to V.$$

Como p manda V en W y como W es G-invariante, entonces p^0 manda V en W. Por otra parte, si $w \in W$, entonces $\rho(g^{-1})w \in W$ y por lo tanto $p \circ \rho(g^{-1})w = \rho(g^{-1})w$ y así

$$\rho(g) \circ p \circ \rho(g^{-1})w = \rho(g) \circ \rho(g^{-1})w = \rho(gg^{-1})w = w,$$

i.e.,

$$p^0(w) = w \qquad \text{para todo } w \in W.$$

Así, $\operatorname{Im} p^0 = W$ y p^0 es una proyección de V en W. Sea $W^0 := \ker p^0$; como $W = \operatorname{Im} p^0$, entonces $V = W \oplus W^0$. Mostraremos que W^0 es G-invariante. En efecto, si $\sigma \in G$, entonces

$$\begin{aligned}
\rho(\sigma) \circ p^0 \circ \rho(\sigma^{-1}) &= \rho(\sigma) \circ \left(\frac{1}{|G|} \sum_{g \in G} \rho(g) \circ p \circ \rho(g^{-1}) \right) \circ \rho(\sigma^{-1}) \\
&= \frac{1}{|G|} \sum_{g \in G} \rho(\sigma)\rho(g) \circ p \circ \rho(g^{-1})\rho(\sigma^{-1}) \\
&= \frac{1}{|G|} \sum_{g \in G} \rho(\sigma g) \circ p \circ \rho(\sigma g)^{-1} \\
&= p^0 \qquad \text{ya que } \sigma g \text{ recorre } G \text{ cuando } g \text{ lo hace.}
\end{aligned}$$

Se sigue que $\rho(\sigma) \circ p^0 = p^0 \circ \rho(\sigma)$ para todo $\sigma \in G$.

Finalmente, si $w \in W^0 = \ker p^0$ y si $\sigma \in G$, entonces $p^0\rho(\sigma)w = \rho(\sigma)p^0w = 0$ y así $\rho(\sigma)w \in \ker p^0 = W^0$, por lo que W^0 es G-invariante. □

Ejemplo 11. En el ejemplo 9 y con la notación de la demostración del teorema 13.2, la proyección $p : V = W \oplus W' \to W$ está determinada por

$$(\dagger) \qquad p(v_\sigma) := \begin{cases} v = \sum_{g \in G} v_g & \text{si } \sigma = 1, \\ 0 & \text{si } \sigma \neq 1. \end{cases}$$

Se sigue que, si $\tau \in G$,

$$p^0 v_\tau = \frac{1}{|G|}\sum_{g\in G}\rho(g)\circ p\circ\rho(g^{-1})v_\tau = \frac{1}{|G|}\sum_{g\in G}\rho(g)p(v_{g^{-1}\tau})$$

$$= \frac{1}{|G|}\rho(\tau)p(v_1) \qquad \text{ya que por } (\dagger) \text{ sólo sobreviven los términos}$$

$$\text{con } g^{-1}\tau = 1, \text{ i.e., con } g = \tau.$$

$$= \frac{1}{|G|}\rho(\tau)\sum_{g\in G} v_g \quad \text{por } (\dagger)$$

$$= \frac{1}{|G|}\sum_{g\in G}\rho(\tau)v_g = \frac{1}{|G|}\sum_{g\in G} v_{\tau g}$$

$$= \frac{1}{|G|}v \quad \text{por definición de } v \text{ en el ejemplo 9.}$$

Por lo tanto,

$$p^0\Big(\sum_{g\in G}\lambda_g v_g\Big) = \sum_{g\in G}\lambda_g p^0(v_g) = \sum_{g\in G}\lambda_g\frac{1}{|G|}v = \frac{1}{|G|}\Big(\sum_{g\in G}\lambda_g\Big)v$$

y así el complemento directo G-invariante de W es

$$W^0 := \ker p^0 = \Big\{\sum_{g\in G}\lambda_g v_g \;:\; \sum_{g\in G}\lambda_g = 0\Big\}.$$

Sumas directas de representaciones. Si $\rho : G \to \mathrm{GL}(V)$ es una representación lineal de grado n de un grupo finito G y si $W, W^0 \subseteq V$ son subespacios G-invariantes tales que $V = W \oplus W^0$, entonces dado un vector $v \in V$ lo podemos escribir, en forma única, como $v = w + w^0$, con $w \in W$ y $w^0 \in W^0$. Ahora, si $\sigma \in G$ es cualquier elemento, entonces

$$\rho(\sigma)v = \rho(\sigma)(w + w^0) = \rho(\sigma)w + \rho(\sigma)w^0$$

y como $w \in W$, $w^0 \in W^0$ y éstos son G-invariantes, entonces $\rho(\sigma)w \in W$ y $\rho(\sigma)w^0 \in W^0$, por lo que la igualdad anterior se puede escribir como

$$\rho(\sigma)v = \rho^W(\sigma)w + \rho^{W^0}(\sigma)w^0,$$

es decir, las subrepresentaciones ρ^W y ρ^{W^0} determinan a la representación ρ. En esta situación, diremos que la representación ρ es la *suma directa* de las subrepresentaciones ρ^W y ρ^{W^0}. Observemos ahora que si $\mathcal{B}$ y $\mathcal{B}^0$ son bases de W y W^0 respectivamente,

entonces $\mathcal{A} = \mathcal{B} \cup \mathcal{B}^0$ es una base de V, y para cada $\sigma \in G$ la matriz asociada a $\rho(\sigma)$ es de la forma

$$[\rho(\sigma)]_{\mathcal{A}} = \begin{pmatrix} [\rho^W(\sigma)]_{\mathcal{B}} & 0 \\ 0 & [\rho^{W^0}(\sigma)]_{\mathcal{B}^0} \end{pmatrix}$$

donde $[\rho^W(\sigma)]_{\mathcal{B}}$ y $[\rho^{W^0}(\sigma)]_{\mathcal{B}^0}$ son las matrices asociadas a $\rho^W(\sigma)$ y $\rho^{W^0}(\sigma)$, respectivamente.

En general, si $V = W_1 \oplus \cdots \oplus W_t$ es una suma directa de subespacios G-invariantes W_i y si $\rho_i = \rho^{W_i}$ son las subrepresentaciones correspondientes, entonces diremos que la representaciónn ρ es la *suma directa* de las subrepresentaciones ρ_i, y la forma matricial tiene la estructura en bloques:

$$[\rho(\sigma)] = \begin{pmatrix} [\rho_1(\sigma)] & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & [\rho_t(\sigma)] \end{pmatrix}.$$

Con esta terminología, el teorema 13.2 nos dice que si $\rho : G \to \mathrm{GL}(V)$ es una representación y si $\rho^W : G \to \mathrm{GL}(W)$ es una subrepresentación, entonces existe otra subrepresentación $\rho^{W^0} : G \to \mathrm{GL}(W^0)$ tal que $\rho = \rho^W \oplus \rho^{W^0}$. Note que lo importante en este teorema es la hipótesis de que V tenga un subespacio G-invariante W no trivial. Si el espacio V es tal que $V \neq 0$ y ningún subespacio propio y no trivial de V es G-invariante, diremos que la representación ρ es *irreducible* o *simple*. Por el teorema 13.2, ésto es equivalente a pedir que V no sea la suma directa de dos subrepresentaciones, excepto por la descomposición trivial $V = V \oplus 0$.

Ejemplo 12. Toda representación de grado 1 es irreducible, ya que los únicos subespacios posibles son el 0 y el total.

Ejemplo 13. Sea G un grupo abeliano finito. Por el teorema de estructura, 7.2, G es una suma directa de grupos cíclicos

$$G = C(n_1) \oplus \cdots \oplus C(n_t)$$

con $n_i | n_{i+1}$ y con $C(n_i) \simeq \mathbb{Z}/n_i\mathbb{Z}$.

Ahora, si $\rho : G \to \mathbb{C}^*$ es una representación de grado 1, entonces ρ está determinada por sus valores en los generadores de G, i.e, en los generadores de los sumandos cíclicos $C(n_i) \simeq \mathbb{Z}/n_i\mathbb{Z}$ de G:

$$e_i := (0, \ldots, 1, \ldots, 0) \in G = C(n_1) \oplus \cdots \oplus C(n_t)$$

(con el 1 en el lugar i). Observe ahora que, como el orden de e_i es n_i, entonces $\rho(e_i)^{n_i} = 1$, por lo que cada $\rho(e_i) \in \mu_{n_i} \subseteq \mathbb{C}^*$ es una raíz n_i-ésima de la unidad. Recíprocamente, para cada elección de una raíz $\omega_i \in \mu_{n_i}$ se tiene la representación

ρ de grado 1 definida, para $(a_1, \ldots, a_t) \in G$, escogiendo las a_i de tal forma que $0 \leq a_i < n_i$, mediante

$$(*) \qquad \rho(a_1, \ldots, a_t) := \omega_1^{a_1} \cdots \omega_t^{a_t}$$

y observamos que hay $n_1 \cdots n_t = |G|$ posibilidades para la elección de las $(\omega_1, \ldots, \omega_t)$ y por lo tanto hay $|G|$ posibles representaciones $(*)$, las cuales son distintas entre sí porque si

$$\rho'(a_1, \ldots, a_t) := \omega_1'^{a_1} \cdots \omega_t'^{a_t}$$

con los $\omega_i' \in \mu_{n_i}$, entonces $\rho = \rho'$ si y sólo si

$$\rho(e_1) = \rho'(e_1), \ldots, \rho(e_t) = \rho'(e_t),$$

lo cual sucede si y sólo si $\omega_1 = \omega_1', \ldots, \omega_t = \omega_t'$.

Hemos así mostrado que, *si G es un grupo abeliano finito, entonces G tiene $|G|$ representaciones de grado 1, no equivalentes entre sí.*

La importancia de las representaciones irreducibles es que éstas son las partículas con las cuales se construyen todas las otras representaciones mediante sumas directas:

TEOREMA 13.3 (Maschke). *Toda representación de un grupo finito es suma directa de representaciones irreducibles.*

Demostración. Sea $\rho : G \to \mathrm{GL}(V)$ una representación de grado $n = \dim_{\mathbb{C}} V$. Haremos inducción sobre n. Si $n = 1$, ρ es irreducible y no hay nada que probar. Supongamos que $n > 1$. Si ρ es irreducible no hay nada que probar. Si ρ es reducible, existe un subespacio G-invariante $W \subseteq V$ con $1 \leq \dim_{\mathbb{C}} W < n$, y por el teorema 13.2, W tiene un complemento G-invariante W^0 tal que $V = W \oplus W^0$ y es claro que $1 \leq \dim_{\mathbb{C}} W^0 < n$. Por hipótesis de inducción ρ^W y ρ^{W^0} se descomponen en sumas directas de irreducibles y así $\rho = \rho^W \oplus \rho^{W^0}$ también se descompone en suma de irreducibles. □

Ejemplo 14. Podríamos preguntarnos si la descomposición anterior es única. La respuesta es negativa, como lo muestra el ejemplo siguiente: la representación

$$\rho : G \to \mathrm{GL}(n, \mathbb{C}) \qquad \text{dada por} \qquad \rho(g) = I_n, \quad \text{para toda } g \in G$$

es tal que todos los subespacios de $\mathbb{C}^n$ son G-invariantes, en particular, para los de dimensión 1, i.e., para las rectas, que son irreducibles. Se sigue que cualquier subespacio unidimensional de $\mathbb{C}^n$ puede formar parte de una descomposición de ρ.

Ejemplo 15. Consideremos la representación regular del grupo cíclico $\mathbb{Z}/n\mathbb{Z}$,

$$\rho : \mathbb{Z}/n\mathbb{Z} \to \mathrm{GL}(V)$$

donde V tiene base $v_0, \ldots, v_{n-1}$ indexada por los elementos de $\mathbb{Z}/n\mathbb{Z}$. Por definición de la representación regular

$$\rho(i)v_j = v_{i+j} \quad \text{donde la suma } i+j \text{ es en } \mathbb{Z}/n\mathbb{Z}, \text{ i.e., es módulo } n.$$

Por el ejemplo 13 hay exactamente n representaciones de grado 1 de $\mathbb{Z}/n\mathbb{Z}$ y para determinar éstas hay que hallar los subespacios unidimensionales invariantes de V. Necesitaremos el lema siguiente:

LEMA 13.4. *Si $W = \langle w \rangle \subseteq V$ es un subespacio unidimensional, i.e., $w \neq 0$, entonces W es $\mathbb{Z}/n\mathbb{Z}$-invariante si y sólo si $\rho(1)w = \lambda w$, para algún $\lambda \in \mathbb{C}^*$.*

Demostración. Si W es invariante, entonces $\rho(1)w \in W = \langle w \rangle$ y así $\rho(1)w = \lambda w$, para algún $\lambda \in \mathbb{C}$, y $\lambda \neq 0$ porque de lo contrario $\rho(1)w = 0$ y así $\rho(1) : W \to W$ sería la transformación lineal 0, en contradicción con el hecho de que es un isomorfismo. Recíprocamente, si $\rho(1)w = \lambda w$, con $\lambda \in \mathbb{C}^*$, entonces para cada $k \in \mathbb{Z}/n\mathbb{Z}$ se tiene que

$$\rho(k)w = \rho(1 + \cdots + 1)w = \rho(1)^k w = \lambda^k w \in \langle w \rangle = W$$

y así W es invariante. □

Del lema anterior se sigue que para detectar cuáles subespacios unidimensionales de V son invariantes, basta detectar cuáles vectores $0 \neq w \in V$ son vectores propios de $\rho(1) : V \to V$. Para ésto, observemos que la matriz de $\rho(1)$ en la base regular $v_0, \ldots, v_{n-1}$ de V está dada por la transpuesta de la matriz de coeficientes en:

$$\begin{array}{rcccccc}
\rho(1)v_0 & = & v_1 & & & & \\
\rho(1)v_1 & = & & v_2 & & & \\
\rho(1)v_2 & = & & & v_3 & & \\
\vdots & & & & & & \\
\rho(1)v_{n-2} & = & & & & & v_{n-1} \\
\rho(1)v_{n-1} & = & v_0 & & & &
\end{array}$$

es decir, la matriz de $\rho(1)$ es:

$$R_1 = \begin{pmatrix} 0 & 0 & \cdots & 0 & 1 \\ 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \vdots & & \ddots & & \vdots \\ 0 & 0 & \cdots & 1 & 0 \end{pmatrix}$$

cuyo polinomio característico es

$$\det(R_1 - \lambda I_n) = \det \begin{pmatrix} -\lambda & 0 & \cdots & 0 & 1 \\ 1 & -\lambda & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \vdots & & \ddots & & \vdots \\ 0 & 0 & \cdots & 1 & -\lambda \end{pmatrix} = (-1)^n\lambda^n + (-1)^{n-1}1^{n-1}$$
$$= \pm(\lambda^n - 1)$$

por lo que sus valores propios son las raíces de $\lambda^n - 1 = 1$, i.e., son las raíces n-ésimas de la unidad, $\lambda_0 = 1$, $\lambda_1 = e^{2\pi i/n}$, $\lambda_2 = \lambda_1^2, \ldots, \lambda_{n-1} = \lambda_1^{n-1}$. Así, los vectores propios w_j correspondientes a los valores propios λ_j, para $0 \leq j < n$, dan lugar a subespacios unidimensionales $W_j = \langle w_j \rangle$ que son $\mathbb{Z}/n\mathbb{Z}$-invariantes. Finalmente recordamos que vectores propios correspondientes a valores propios distintos son linealmente independientes y por lo tanto los w_j constituyen una base de V y así $\rho = \rho_0 \oplus \cdots \oplus \rho_{n-1}$, con los ρ_j las subrepresentaciones correspondientes a W_j.

TEOREMA 13.5 (Lema de Schur). *Sean $\rho_1 : G \to \mathrm{GL}(V_1)$ y $\rho_2 : G \to \mathrm{GL}(V_2)$ dos representaciones irreducibles de G y sea $f : V_1 \to V_2$ una transformación lineal tal que $\rho_2(g) \circ f = f \circ \rho_1(g)$, para todo $g \in G$. Entonces,*

(1) *Si ρ_1 y ρ_2 no son isomorfas, entonces $f = 0$.*

(2) *Si $\rho_1 = \rho_2$ (en particular, $V_1 = V_2$), entonces f es una homotecia, i.e., es un múltiplo escalar de la identidad, $f = \lambda \,\mathrm{id}_V$, con $\lambda \in \mathbb{C}$.*

Demostración. Si $f = 0$ no hay nada que probar. Supongamos ahora que $f \neq 0$ y sea $W_1 \subseteq V_1$ el núcleo de f. Si $w \in W_1$ es cualquier vector, como $f \circ \rho_1(g)w = \rho_2(g) \circ f(w) = 0$, entonces $\rho_1(g)w \in \ker f = W_1$ y así W_1 es ρ_1-invariante (i.e., G-invariante bajo ρ_1). Como V_1 es simple, entonces $W_1 = 0$ ó $W_1 = V_1$. Si $W_1 = V_1$, entonces $f = 0$, lo cual contradice la suposición de que $f \neq 0$. Se sigue que $W_1 = 0$ y por lo tanto f es inyectiva. Pongamos ahora $W_2 = \mathrm{Im}\, f \subseteq V_2$. Si $w \in W_2$, entonces $w = f(v)$ con $v \in V_1$ y así $\rho_2(g)w = \rho_2(g)f(v) = f\rho_1(g)v \in \mathrm{Im}\, f = W_2$, por lo que W_2 es ρ_2-invariante (i.e., G-invariante bajo ρ_2). Como V_2 es simple, entonces $W_2 = 0$ ó $W_2 = V_2$. El caso $W_2 = 0$ no es posible porque implicaría que $f = 0$. Se sigue que $W_2 = V_2$ y por lo tanto f es suprayectiva. Hemos así mostrado que si $f \neq 0$, entonces f es un isomorfismo, lo cual prueba (1).

Para (2), supongamos ahora que $V = V_1 = V_2$ y $\rho_1 = \rho_2$. Sea λ un valor propio de f (el cual siempre existe porque estamos considerando espacios vectoriales sobre $\mathbb{C}$) y pongamos $\tilde{f} := f - \lambda \,\mathrm{id}_V$. Como λ es valor propio de f, entonces $\ker \tilde{f} \neq 0$ (ya que

existe un vector propio no nulo). Por otra parte,

$$\begin{aligned}\rho_2(g)\circ\widetilde{f} &= \rho_2(g)(f-\lambda\,\mathrm{id}_V) = \rho_2(g)f - \lambda\rho_2(g)\\ &= f\rho_1(g) - \lambda\rho_1(g) \qquad \text{ya que } \rho_2(g)\circ f = f\circ\rho_1(g) \text{ y } \rho_1 = \rho_2\\ &= (f-\lambda\,\mathrm{id}_V)\rho_1(g)\\ &= \widetilde{f}\circ\rho_1(g)\end{aligned}$$

y así podemos aplicar la parte (1) a $\widetilde{f}$, y como $\ker\widetilde{f} \neq 0$, entonces $\widetilde{f} = 0$ por (1). Se sigue que $f - \lambda\,\mathrm{id}_V = 0$, como se quería. □

Ejemplo 16. Usando el lema de Schur podemos completar lo obtenido al final del ejemplo 14: supongamos que $\rho : G \to \mathrm{GL}(V)$ es una representación irreducible del grupo abeliano finito G y sea $\sigma \in G$. Como G es abeliano, entonces, para todo $g \in G$,

$$\rho(\sigma)\rho(g) = \rho(\sigma g) = \rho(g\sigma) = \rho(g)\rho(\sigma)$$

por lo que la función lineal $\rho(\sigma) : V \to V$ satisface la hipótesis del lema de Schur y así $\rho(\sigma)$ es un múltiplo escalar de la identidad, $\rho(\sigma) = \lambda\,\mathrm{id}_V$. Por lo tanto, si $W \subseteq V$ es cualquier subespacio vectorial, entonces para todo $\sigma \in G$ y para todo $w \in W$, se tiene que $\rho(\sigma)w = \lambda\,\mathrm{id}_V(w) = \lambda w \in W$, es decir, W es G-invariante, pero como V es irreducible ésto sólo es posible si $\dim_{\mathbb{C}} V = 1$. Hemos así probado:

COROLARIO 13.6. *Si G es un grupo abeliano finito, entonces todas sus representaciones irreducibles son de grado* 1.

□

Notas. (1) En el caso importante cuando el grupo G es *finito* y cuando V es un espacio vectorial sobre los complejos y de dimensión finita, el estudio de las representaciones complejas de G se inició a finales del siglo XIX con los trabajos de Frobenius con la intención de obtener resultados en la teoría de grupos finitos que, como se vio posteriormente, no eran accesibles con los métodos desarrollados previamente. La pequeña introducción a la teoría de representaciones de grupos que vimos en este capítulo se debe esencialmente a Frobenius [36], excepto por el teorema de Maschke y el lema de Schur, que puede verse en [52].

(2) En este capítulo sólo consideramos espacios vectoriales sobre $\mathbb{C}$, pero mucho de lo que desarrollamos permanece válido para cualquier campo K algebraicamente cerrado y cuya característica no divida al orden $|G|$ del grupo.

EJERCICIO 1. Demuestre que la correspondencia entre operadores lineales invertibles en un $\mathbb{C}$-espacio vectorial de dimensión finita n y matrices complejas invertibles $n \times n$, es un isomorfismo de grupos $\mathrm{GL}(V) \simeq \mathrm{GL}(n, \mathbb{C})$.

EJERCICIO 2. Muestre que las correspondencias usadas en la demostración del teorema 13.1 son inversas una de la otra.

EJERCICIO 3. En el ejemplo 5, demuestre que las matrices, de la representación regular de un grupo finito, consisten de ceros y unos.

EJERCICIO 4. Demuestre que todo grupo finito de orden $|G| = n$ es isomorfo a un subgrupo de $\mathrm{GL}(n, \mathbb{C})$. *Sugerencia*: vea el ejemplo 7 y piense en el núcleo de $\rho : S_n \to \mathrm{GL}(n, \mathbb{C})$.

EJERCICIO 5. Si G es un grupo finito y $[G : G]$ es su subgrupo conmutador, por los ejercicios 11 y 12 del capítulo 5, $G/[G : G]$ es el mayor cociente abeliano de G. Demuestre que hay una biyección entre la familia de las representaciones de grado 1 de G y la familia de las representaciones de grado 1 de $G/[G : G]$. Concluya que G tiene exactamente $|G/[G : G]|$ representaciones de grado 1. *Sugerencia*: use el homomorfismo canónico $\pi : G \to G/[G : G]$ para dar la correspondencia fácil y también para la otra, usando además que si $\rho : G \to \mathbb{C}^*$ entonces ρ se anula en el subgrupo $[G : G]$ y así el primer teorema de isomorfismo de Noether implica la existencia de $\rho' : G/[G : G] \to \mathbb{C}^*$.

EJERCICIO 6. Concluya que S_n, para $n \geq 3$, sólo tiene dos representaciones de grado 1. Calcule éstas. *Sugerencia*: vea la proposición 5.14.

EJERCICIO 7. Defina $\rho : S_4 \to \mathrm{GL}(3, \mathbb{C})$, en los generadores de S_4, (vea 4.15), mediante

$$\rho(1\,2) := \begin{pmatrix} -1 & 0 & 0 \\ -1 & 1 & 0 \\ -1 & 0 & 1 \end{pmatrix} \quad \text{y} \quad \rho(1\,2\,3\,4) := \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}$$

y extienda ρ a una representación de grado 3 de S_4.

EJERCICIO 8. Defina $\rho' : S_4 \to \mathrm{GL}(3, \mathbb{C})$, en los generadores de S_4, (vea 4.15), mediante

$$\rho'(1\,2) := \begin{pmatrix} 1 & 0 & 0 \\ 1 & -1 & 0 \\ 1 & 0 & -1 \end{pmatrix} \quad \text{y} \quad \rho'(1\,2\,3\,4) := \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}$$

y extienda ρ' a una representación de grado 3 de S_4.

EJERCICIO 9. ¿Son ρ y ρ' isomorfas?

EJERCICIO 10. Calcule explícitamente la representación por permutaciones (vea el ejemplo 7) del grupo S_3.

EJERCICIO 11. Usando el ejercicio 10 para ver la forma que tienen las matrices $\rho(\sigma)$, muestre que la representación por permutaciones de S_3 es reducible.

EJERCICIO 12. Si $n \geq 2$, demuestre que la representación por permutaciones de S_n es reducible.

EJERCICIO 13. Si $\rho : S_n \to \mathrm{GL}(n, \mathbb{C})$ es la representación por permutaciones del grupo simétrico S_n, demuestre que para toda $\sigma \in S_n$ la matriz $\rho(\sigma)$ se obtiene permutando las columnas de la matriz identidad I_n de acuerdo a σ (en la notación del ejercicio 12 del capítulo 6, $\rho(\sigma) = I_n^{\sigma}$).

EJERCICIO 14. Una representación $\rho : G \to \mathrm{GL}(V)$ se dice que es *fiel* si ρ es inyectiva. ¿Bajo qué condiciones las representaciones siguientes son fieles?

(i) La representación trivial de un grupo G.
(ii) La representación regular de un grupo G.
(iii) La representación por permutaciones de S_n.
(iv) La representación signo de S_n.

EJERCICIO 15. Si $\rho : G \to \mathrm{GL}(V)$ es una representación de G y $N \lhd G$ es tal que $N \subseteq \ker \rho$, defina $\overline{\rho} : G/N \to \mathrm{GL}(V)$ mediante $\overline{\rho}(gN) := \rho(g)$.

(i) Demuestre que $\overline{\rho}$ es una representación de G/N.
(ii) Demuestre que $\overline{\rho}$ es irreducible si y sólo si ρ lo es.
(iii) Si $N = \ker \rho$, demuestre que $\overline{\rho}$ es fiel.

EJERCICIO 16. Se puede invertir la construcción del ejercicio 15: si $N \lhd G$ es cualquier subgrupo normal de G y si $\widehat{\rho} : G/N \to \mathrm{GL}(V)$ es una representación de G/N, defina la función $\rho : G \to \mathrm{GL}(V)$ mediante $\rho(g) := \widehat{\rho}(gN)$.

(i) Demuestre que ρ es una representación de G.
(ii) Demuestre que si $\widehat{\rho}$ es fiel, entonces el núcleo de ρ es N.
(ii) Demuestre que $\widehat{\rho}$ es irreducible si y sólo si ρ lo es.

EJERCICIO 17. Sea $\rho : G \to \mathrm{GL}(n, \mathbb{C})$ una representación.

(i) La composición $\delta : G \xrightarrow{\rho} \mathrm{GL}(n, \mathbb{C}) \xrightarrow{\det} \mathrm{GL}(1, \mathbb{C})$ es una representación de grado 1. Muestre que $G/\ker \delta$ es abeliano.
(ii) Suponga que $\delta(g) = -1$ para algún $g \in G$. Demuestre que G tiene un subgrupo normal de índice 2.

EJERCICIO 18. Demuestre que $\rho : G \to \mathrm{GL}(V)$ es fiel si y sólo si $G \simeq \mathrm{Im}\, \rho$.

Capítulo **14**

Caracteres de grupos finitos

DADA UNA MATRIZ $A = (a_{ij})$ DE TAMAÑO $n \times n$ y con entradas en $\mathbb{C}$, su *traza* es el escalar

$$\mathrm{Tr}(A) = \sum_{i=1}^{n} a_{ii}.$$

Recordemos que si A y B son dos matrices $n \times n$, entonces $\mathrm{Tr}(AB) = \mathrm{Tr}(BA)$. Consecuentemente, si M, Q son matrices $n \times n$, con Q una matriz invertible, poniendo $A = QM$ y $B = Q^{-1}$, se tiene que $AB = QMQ^{-1}$ y $BA = M$, por lo que

$$(*) \qquad \mathrm{Tr}(QMQ^{-1}) = \mathrm{Tr}(M).$$

Una consecuencia de esta igualdad es que, si $T : V \to V$ es un operador lineal en un espacio vectorial de dimensión n, podemos definir la *traza del operador* T usando la matriz asociada a T en cualquier base de V, porque las matrices asociadas a T en dos bases cualesquiera de V son conjugadas y entonces podemos aplicar $(*)$.

Ahora, si $\rho : G \to \mathrm{GL}(V)$ es una representación de grado n de un grupo finito G, para cada $g \in G$ sea $\rho(g) : V \to V$ el isomorfismo correspondiente; por las observaciones previas podemos considerar su traza $\mathrm{Tr}(\rho(\sigma)) \in \mathbb{C}$. Se tiene así una función

$$\chi : G \to \mathbb{C} \qquad \text{definida mediante} \qquad \chi(g) := \mathrm{Tr}(\rho(g))$$

a la cual se le llama el *carácter* de la representación ρ. Para denotar su dependencia de ρ, algunas veces denotaremos a χ como χ_ρ. Si n es el grado de la representación ρ, diremos que el carácter χ_ρ es un *carácter de grado n*. El apelativo *carácter* proviene del hecho, que probaremos en 14.7, que χ_ρ *caracteriza* a la representación ρ, en el sentido de que dos representaciones con el mismo carácter son isomorfas. De ahora en adelante denotaremos con 1 a la identidad de un grupo G.

TEOREMA 14.1. *Sea G un grupo finito y sea χ el carácter de una representación $\rho : G \to \mathrm{GL}(V)$ de grado n. Entonces,*

(0) *El operador $\rho(g) : V \to V$ es diagonalizable, para todo $g \in G$.*

(1) $\chi(1) = n$.

(2) $\chi(tgt^{-1}) = \chi(g)$, *para todo $g, t \in G$.*

(3) $\chi(g)$ *es la suma, con multiplicidades, de los valores propios de* $\rho(g)$.

(4) $\chi(g)$ *es la suma de* n *raíces* k*-ésimas de la unidad, donde* k *es el orden de* g.

(5) $\chi(g^{-1}) = \overline{\chi(g)}$.

(6) $|\chi(g)| \leq n = \chi(1)$. *Aquí* 1 *es la identidad de* G.

(7) $\ker \rho = \{g \in G : \chi(g) = \chi(1)\}$.

Demostración. (0): Sea $g \in G$ de orden k y consideremos el subgrupo cíclico $H = \langle g \rangle \subseteq G$. La restricción de ρ a H es una representación $\rho : H \hookrightarrow G \to \mathrm{GL}(V)$ de H. Usando el teorema de Maschke (13.3) sea $V = W_1 \oplus \cdots \oplus W_r$ una descomposición de $\rho : H \to \mathrm{GL}(V)$ en irreducibles. Como H es abeliano, por el corolario 13.6 cada W_i es unidimensional, digamos $W_i = \langle u_i \rangle$ y así $r = n$. Ahora, si $\rho_i : H \to \mathrm{GL}(W_i) \simeq \mathrm{GL}(1, \mathbb{C}) \simeq \mathbb{C}^*$ es la subrepresentación correspondiente, por el ejemplo 1 del capítulo 13, $\rho_i(g)$ es una raíz k-ésima de la unidad, digamos ω^{e_i}, con $\omega = \exp(2\pi i/k)$ una raíz primitiva. Entonces, $\rho_i(g)u_i = \omega^{e_i}u_i$ y por lo tanto, para la base $\{u_1, \ldots, u_r\}$ de V, como $\rho = \rho_1 \oplus \cdots \oplus \rho_n$, entonces

$$[\rho(g)] = \begin{pmatrix} [\rho_1(g)] & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & [\rho_n(g)] \end{pmatrix} = \begin{pmatrix} \omega^{e_1} & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & \omega^{e_n} \end{pmatrix},$$

que es lo que queríamos probar.

(1): Como $\rho(1) = \mathrm{id}_V$, entonces $[\rho(1)] = I_n$ y así $\chi(1) = \mathrm{Tr}(I_n) = n$.

(2): Como $\rho(tgt^{-1}) = \rho(t)\rho(g)\rho(t)^{-1}$, el resultado es consecuencia de la igualdad $\mathrm{Tr}(QAQ^{-1}) = \mathrm{Tr}(A)$.

(3): Como $\rho(g)$ es diagonalizable, su traza es la suma de sus valores propios.

(4): Si k es el orden de g, por la parte (0) en la diagonal de $[\rho(g)]$ aparecen raíces k-ésimas de la unidad.

(5): Los valores propios del operador $\rho(g^{-1}) : V \to V$ son los inversos λ_i^{-1} de los valores propios λ_i de $\rho(g) : V \to V$, y como por (4) las λ_i son raíces de la unidad, entonces $\lambda_i^{-1} = \overline{\lambda_i}$, por lo que

$$\chi(g^{-1}) = \sum_i \overline{\lambda_i} = \overline{\sum_i \lambda_i} = \overline{\chi(g)}.$$

(6): Por (4), $\chi(g) = \sum_{i=1}^n \lambda_i$, con los λ_i raíces de la unidad. De la desigualdad del triángulo se sigue que

$$|\chi(g)| \leq \sum_{i=1}^n |\lambda_i| \leq n \quad \text{ya que } |\lambda_i| = 1.$$

(7): Si g es tal que $\chi(g) = \chi(1) = n$, como $\chi(g)$ es la suma de sus n valores propios y cada uno de éstos tiene valor absoluto 1, entonces cada uno de éstos debe ser 1 y por lo tanto la matriz de $\rho(g)$ debe ser I_n y así $g \in \ker \rho$. Recíprocamente, si $g \in \ker \rho$, entonces $\rho(g) = \mathrm{id}_V$ y así su matriz es I_n, por lo que $\chi(g) = \mathrm{Tr}(I_n) = n = \chi(1)$. □

PROPOSICIÓN 14.2. *Si $\rho_1 : G \to \mathrm{GL}(V_1)$ y $\rho_2 : G \to \mathrm{GL}(V_2)$ son dos representaciones del grupo finito G, y si χ_1 y χ_2 son sus caracteres, entonces*

$$\chi_{\rho_1 \oplus \rho_2} = \chi_1 + \chi_2.$$

Demostración. Si $V = V_1 \oplus V_2$ y si $\mathcal{B}_1$ y $\mathcal{B}_2$ son bases de V_1 y V_2, respectivamente, entonces $\mathcal{B}_1 \cup \mathcal{B}_2$ es base de V y la matriz asociada a $(\rho_1 \oplus \rho_2)(g)$ es de la forma

$$[(\rho_1 \oplus \rho_2)(g)]_{\mathcal{B}} = \begin{pmatrix} [\rho_1(g)]_{\mathcal{B}_1} & 0 \\ 0 & [\rho_2(g)]_{\mathcal{B}_2} \end{pmatrix},$$

por lo que

$$\chi_{\rho_1 \oplus \rho_2}(g) = \mathrm{Tr}[(\rho_1 \oplus \rho_2)(g)]_{\mathcal{B}} = \mathrm{Tr}[\rho_1(g)]_{\mathcal{B}_1} + \mathrm{Tr}[\rho_2(g)]_{\mathcal{B}_2} = \chi_1(g) + \chi_2(g).$$

□

Ejemplo 1. Si $\rho : G \to \mathbb{C}^*$ es la representación trivial $\rho(g) = 1$, para todo $g \in G$, su carácter está dado por $\chi(g) := \mathrm{Tr}[\rho(g)] = 1$, para todo $g \in G$. A éste carácter lo llamaremos el *carácter principal* de G y lo denotaremos por χ_1.

Ejemplo 2. Si $\rho : G \to \mathrm{GL}(V)$ es la representación regular de G, $n = |G| = \dim_{\mathbb{C}} V$, y si el espacio V tiene como base a $\{v_g\}_{g \in G}$, por definición de la representación regular se tiene que $\rho(\sigma)v_g = v_{\sigma g}$ y notamos que $\rho(\sigma)v_g = v_g$ si y sólo si $\sigma g = g$, i.e., si y sólo si $\sigma = 1$. Así, si $[\rho(\sigma)]$ es la matriz asociada a $\rho(\sigma)$ en la base regular, entonces:

(1) Si $\sigma \neq 1$ (el neutro de G), la diagonal de $[\rho(\sigma)]$ consiste de ceros.

(2) Si $\sigma = 1$, la diagonal de $[\rho(1)]$ consiste de unos.

Se sigue que el carácter χ de la representación regular está dado por:

$$\chi(\sigma) = \begin{cases} 0 & \text{si } \sigma \neq 1, \\ |G| & \text{si } \sigma = 1. \end{cases}$$

Ejemplo 3. El ejemplo anterior se puede generalizar considerando un grupo (finito) G que actúa sobre un conjunto (finito) Y, lo cual define la *representación por permutaciones* (vea el ejemplo 7 del capítulo 13) $\phi : G \to \mathrm{GL}(V)$, donde el espacio vectorial V tiene una base $\{v_x : x \in Y\}$ indexada por Y y si $\sigma \in G$, $\phi(\sigma)v_x := v_{\sigma x}$, donde σx es la acción de σ en x. Notamos entonces que $\phi(\sigma)v_x = v_x$ si y sólo si $\sigma x = x$, i.e., si y sólo si $x \in Y^{\sigma}$. Es decir, en la diagonal de la matriz asociada a $\phi(\sigma)$ se tiene

un 1 por cada $x \in Y^\sigma$ y por lo tanto la traza $\mathrm{Tr}[\phi(\sigma)]$ cuenta los puntos $x \in Y^\sigma$, i.e., el carácter χ de la representación por permutaciones de G en Y está dado por

$$\chi(\sigma) = |Y^\sigma|.$$

Ejemplo 4. Si $G = \mathbb{Z}/n\mathbb{Z}$, en el ejemplo 15 del capítulo 13 vimos que la representación regular ρ de $\mathbb{Z}/n\mathbb{Z}$ es la suma directa de las representaciones ρ_ω de grado 1, con $\omega \in \mu_n$, definidas en el ejemplo 3 del capítulo 13, para $j \in \mathbb{Z}/n\mathbb{Z}$, como

$$\rho_\omega(j) := \omega^j.$$

Entonces, si χ_ω es el carácter de ρ_ω, se tiene que

$$\chi_\omega(j) = \omega^j$$

y por lo tanto, si χ es el carácter de la representación regular ρ, entonces por 14.2,

$$\chi(j) = \sum_{\omega \in \mu_n} \chi_\omega(j) = \sum_{\omega \in \mu_n} \omega^j,$$

que, comparando con el resultado general del ejemplo 2 anterior nos da

$$\sum_{\omega \in \mu_n} \omega^j = 0 \quad \text{para } 0 < j < n.$$

El resultado siguiente es un corolario del lema de Schur 13.5 y nos será útil para analizar la ortogonalidad de los caracteres irreducibles de un grupo:

COROLARIO 14.3. *Sean $\rho_1 : G \to \mathrm{GL}(V_1)$ y $\rho_2 : G \to \mathrm{GL}(V_2)$ dos representaciones irreducibles de G y sea $h : V_1 \to V_2$ una transformación lineal arbitraria. Pongamos*

$$h^0 := \frac{1}{|G|} \sum_{g \in G} \rho_2(g)^{-1} \circ h \circ \rho_1(g).$$

(1) *Si ρ_1 y ρ_2 no son isomorfas, entonces $h^0 = 0$.*

(2) *Si $\rho_1 = \rho_2$ (en particular, $V_1 = V_2 =: V$), entonces h^0 es una homotecia de razón $\lambda = (1/n)\mathrm{Tr}(h)$, donde $n = \dim_{\mathbb{C}} V$.*

Demostración. La transformación lineal h^0 satisface $\rho_2(g) \circ h^0 = h^0 \circ \rho_1(g)$ ya que

$$\begin{aligned}
\rho_2(\tau)^{-1} h^0 \rho_1(\tau) &= \frac{1}{|G|} \sum_{g \in G} \rho_2(\tau)^{-1} \rho_2(g)^{-1} \circ h \circ \rho_1(g) \rho_1(\tau) \\
&= \frac{1}{|G|} \sum_{g \in G} \rho_2(g\tau)^{-1} \circ h \circ \rho_1(g\tau) \\
&= h^0.
\end{aligned}$$

Podemos entonces aplicar el lema de Schur a $f = h^0$ y concluir (1) y (2), excepto por la identificación del escalar λ. Ahora, como $\rho_1 = \rho_2$, entonces

$$\mathrm{Tr}(h^0) = \frac{1}{|G|}\sum_{g\in G}\mathrm{Tr}(\rho_1(g)^{-1}\circ h\circ\rho_1(g)) = \frac{1}{|G|}\sum_{g\in G}\mathrm{Tr}(h) = \mathrm{Tr}(h)$$

y como $h^0 = \lambda\,\mathrm{id}_V$, entonces $\mathrm{Tr}(h^0) = \lambda\mathrm{Tr}(\mathrm{id}_V) = n\lambda$, por lo que $n\lambda = \mathrm{Tr}(h)$ y así $\lambda = (1/n)\mathrm{Tr}(h)$. □

Ortogonalidad de caracteres. Si $\phi, \psi : G \to \mathbb{C}$ son dos funciones, pongamos

$$\langle\phi,\psi\rangle := \frac{1}{|G|}\sum_{g\in G}\phi(g)\overline{\psi(g)}$$

y observemos que éste es un producto interno, ya que:

(1) Es lineal en ϕ, i.e., es aditivo y saca escalares.

(2) Es aditivo en ψ.

(3) $\langle\psi,\phi\rangle = \overline{\langle\phi,\psi\rangle}$.

(4) Saca escalares conjugados en ψ. (Se sigue de 3 y 1).

(5) $\langle\phi,\phi\rangle > 0$ para toda $\phi \neq 0$.

En particular, si $\phi, \psi : G \to \mathbb{C}$ son caracteres, como $\overline{\psi(g)} = \psi(g)^{-1}$, por 14.1, la definición del producto interior se vuelve

$$\langle\phi,\psi\rangle = \frac{1}{|G|}\sum_{g\in G}\phi(g)\psi(g^{-1})$$

y observamos que $\sum_{g\in G}\phi(g)\overline{\psi(g)} = \sum_{g\in G}\phi(g^{-1})\psi(g)$, ya que g^{-1} recorre G cuando g lo hace. Se sigue que

$$\langle\phi,\psi\rangle = \langle\psi,\phi\rangle$$

cuando ϕ y ψ son caracteres.

TEOREMA 14.4. *Sea G un grupo finito.*

(1) *Si χ y χ' son caracteres de dos representaciones irreducibles no isomorfas de G, entonces son ortogonales, i.e., $\langle\chi,\chi'\rangle = 0$.*

(2) *Si χ es el carácter de una representación irreducible de G, entonces es de norma 1, i.e., $\langle\chi,\chi\rangle = 1$.*

Demostración. (1) Sean $\rho : G \to \mathrm{GL}(V)$ y $\rho' : G \to \mathrm{GL}(V')$ dos representaciones irreducibles de G, con caracteres χ y χ', respectivamente. Sean $[\rho(g)] = (a_{ij})$ y $[\rho'(g)] = (a'_{k\ell})$ matrices correspondientes. Si $h : V \to V'$ es cualquier aplicación lineal con matriz asociada $[h] = (x_{st})$ en las bases de V y V' usadas anteriormente,

como la matriz de $\rho(g^{-1})$ es de la forma $(a_{ij}(g^{-1}))$, entonces para el h^0 del corolario anterior su matriz asociada es

$$[h^0] = \frac{1}{|G|}\sum_{g\in G}[\rho(g^{-1})][h][\rho'(g)]$$

(ya que la matriz de una suma de aplicaciones lineales, es la suma de las matrices, y la matriz de una composición es el producto de las matrices), y así, los coeficientes h^0_{ij} de $[h^0]$ son

$$(*) \qquad h^0_{ij} = \frac{1}{|G|}\sum_{g\in G}\sum_{k,t} a_{ik}(g^{-1})x_{kt}a'_{tj}(g).$$

Ahora, como ρ y ρ' no son isomorfas, por el corolario anterior se tiene que $h^0 = 0$ y así las $h^0_{ij} = 0$ para todo i, j. Se sigue que $(*)$ es un sistema de ecuaciones lineales en las variables x_{st} que se anula para cualquier $h : V \to V$, i.e., para todos los valores de x_{st}. Por lo tanto sus coeficientes tienen que ser todos cero, i.e.,

$$(\dagger) \qquad \frac{1}{|G|}\sum_{g\in G,\, k,t} a_{ik}(g^{-1})a'_{tj}(g) = 0 \quad \text{para todo } i, j, k, t.$$

Ahora, como $\chi(g) = \sum_i a_{ii}(g)$ y $\chi'(g) = \sum_j a'_{jj}(g)$, entonces

$$\begin{aligned}\langle \chi, \chi' \rangle &= \langle \sum_i a_{ii}, \sum_j a'_{jj} \rangle = \sum_{i,j}\langle a_{ii}, a'_{jj}\rangle \\ &= \sum_{i,j}\frac{1}{|G|}\sum_{g\in G} a_{ii}(g^{-1})a'_{jj}(g) \quad \text{por definición de } \langle\ ,\ \rangle \\ &= \frac{1}{|G|}\sum_{i,j,g\in G} a_{ii}(g^{-1})a'_{jj}(g) \\ &= 0, \quad \text{por } (\dagger),\end{aligned}$$

lo cual prueba la parte (1).

(2) Con la misma notación para $\rho = \rho'$ y h, sólo que en este caso tenemos, por el corolario anterior, que $h^0 = \lambda\,\mathrm{id}_V$, para un escalar λ de la forma $\lambda = (1/n)\mathrm{Tr}(h)$, con $n = \dim_{\mathbb{C}} V$, por lo que

$$h^0_{ij} = \begin{cases} 0 & i \neq j, \\ \lambda & i = j, \end{cases}$$

i.e., $h^0_{ij} = \lambda\delta_{ij}$, la delta de Kronecker, y como λ es de la forma

$$\lambda = \frac{1}{n}\mathrm{Tr}(h) = \frac{1}{n}\sum_k x_{kk} = \frac{1}{n}\sum_{s,t} x_{st}\delta_{st}$$

entonces

$$h_{ij}^0 = \lambda\delta_{ij} = \frac{1}{n}\sum_{st} x_{st}\delta_{st}\delta_{ij}$$

por lo que la igualdad (*) se vuelve

$$\frac{1}{n}\sum_{s,t} x_{st}\delta_{st}\delta_{ij} = \frac{1}{|G|}\sum_{i,s,t,j,g\in G} a_{is}(g^{-1})x_{st}a_{tj}(g)$$

e igualando los coeficientes de las variables x_{st} se obtiene que

$$(**) \qquad \frac{1}{|G|}\sum_{g\in G} a_{is}(g^{-1})a_{tj}(g) = \frac{1}{n}\delta_{st}\delta_{ij} = \begin{cases} \frac{1}{n} & \text{si } i = j \text{ y } s = t, \\ 0 & \text{en cualquier otro caso,} \end{cases}$$

y como $\chi(g) = \sum_i a_{ii}(g)$, entonces

$$\begin{aligned} \langle \chi, \chi \rangle &= \langle \sum_i a_{ii}, \sum_j a_{jj} \rangle = \sum_{i,j} \langle a_{ii}, a_{jj} \rangle \\ &= \sum_{i,j} \frac{1}{|G|} \sum_{g\in G} a_{ii}(g^{-1})a_{jj}(g) \quad \text{por definición de } \langle\ ,\ \rangle \\ &= \sum_{i,j} \frac{1}{n}\delta_{ij} \quad \text{por } (**) \\ &= \sum_{i=1}^{n} \frac{1}{n} \\ &= 1, \end{aligned}$$

como se quería. □

Observación. Note que la parte 2 del teorema es una condición necesaria para que una representación ρ sea irreducible: se requiere que $\langle \chi_\rho, \chi_\rho \rangle = 1$. Después de unos ejemplos y corolarios, veremos en 14.7 que la condición anterior también es suficiente.

Ejemplo 5. Si $G \neq 1$ es un grupo finito de orden n, sea $\rho : G \to \mathrm{GL}(V)$ la representación regular de G y sea χ su carácter. Por el ejemplo 2, $\chi(g) = 0$, si $g \neq 1$, y $\chi(1) = n$, por lo que

$$\langle \chi, \chi \rangle = \frac{1}{n}\sum_{g\in G} \chi(g)\chi(g^{-1}) = \frac{1}{n}\chi(1)\chi(1) = \frac{1}{n}n \cdot n = n \neq 1,$$

y por lo tanto la representación regular de grado $n > 1$ no es irreducible, algo que está implícito en el ejemplo 9 del capítulo 13.

COROLARIO 14.5. *Sea G un grupo finito y sea $\rho : G \to \mathrm{GL}(V)$ una representación con carácter χ. Supongamos que la representación se descompone en suma directa de irreducibles como*

$$V = W_1 \oplus \cdots \oplus W_k.$$

Si W es una representación irreducible de G con carácter ψ, entonces $\langle \chi, \psi \rangle$ es un entero que es igual al número de W_i isomorfas a W. Se sigue que el número de W_i isomorfas a W no depende de la descomposición de V.

Demostración. Si χ_i es el carácter de W_i, por 14.2 se tiene que $\chi = \chi_1 + \cdots + \chi_k$, por lo que

$$(*) \qquad \langle \chi, \psi \rangle = \langle \chi_1 + \cdots + \chi_k, \psi \rangle = \langle \chi_1, \psi \rangle + \cdots + \langle \chi_k, \psi \rangle$$

y por el teorema anterior

$$\langle \chi_i, \psi \rangle = \begin{cases} 1 & \text{si } W_i \text{ es isomorfo a } W, \\ 0 & \text{si } W_i \text{ no es isomorfo a } W, \end{cases}$$

por lo que la suma $(*)$ cuenta los W_i isomorfos a W. Para la segunda afirmación del corolario, note que el número $\langle \chi_i, \psi \rangle$ no depende de la descomposición. □

Observación. En el corolario anterior, diremos que $\langle \chi, \psi \rangle$ es el *número de veces que W ocurre en la descomposición en irreducibles de V.*

COROLARIO 14.6. *Dos representaciones ρ_1 y ρ_2 de G, son isomorfas si y sólo si sus caracteres son iguales.*

Demostración. Si $\rho_1 : G \to \mathrm{GL}(V)$ y $\rho_2 : G \to \mathrm{GL}(V')$ son isomorfas, existe un isomorfismo lineal $f : V \to V'$ tal que $f\rho_1(g) = \rho_2(g)f$, para todo $g \in G$. Se sigue que $f\rho_1(g)f^{-1} = \rho_2(g)$ y por lo tanto

$$\chi_1(g) = \mathrm{Tr}(\rho_1(g)) = \mathrm{Tr}(f\rho_1(g)f^{-1}) = \mathrm{Tr}(\rho_2(g)) = \chi_2(g),$$

para todo $g \in G$, y así $\chi_1 = \chi_2$. Recíprocamente, si $\chi_1 = \chi_2$, el corolario anterior nos dice que en este caso ρ_1 y ρ_2 contienen, cada una, una representación irreducible el mismo número de veces. □

Observaciones. (1) Este corolario nos dice que, en efecto, el carácter de una representación determina o caracteriza a la representación.
(2) Los corolarios anteriores también nos dicen que el estudio de las representaciones de un grupo se reduce al estudio de los caracteres del mismo.
(3) Si $\rho : G \to \mathrm{GL}(V)$ es una representación de grado n con carácter χ, supongamos que $W_1, \ldots, W_r$ son todos los irreducibles no isomorfos que aparecen en una descomposición de ρ. Pongamos $m_i := \langle \chi, \chi_i \rangle$, donde χ_i es el carácter de W_i, recordando

de 14.5 que los m_i son enteros ≥ 0, y denotemos con m_iW_i a la suma directa de W_i consigo mismo m_i veces, i.e.,

$$m_iW_i := \overbrace{W_i \oplus \cdots \oplus W_i}^{m_i}$$

(con $0W_i := 0$) Al entero m_i lo llamaremos la *multiplicidad* de W_i. Entonces,

$$V = m_1W_1 \oplus \cdots \oplus m_rW_r$$

y el carácter χ de ρ es una combinación lineal de los caracteres irreducibles $\chi_1, \ldots, \chi_r$, con coeficientes enteros ≥ 0:

$$\chi = m_1\chi_1 + \cdots + m_r\chi_r.$$

COROLARIO 14.7. *Si χ es el carácter de una representación V de G, entonces*

(1) $\langle \chi, \chi \rangle = \sum_{i=1}^{r} m_i^2$.

(2) $\langle \chi, \chi \rangle > 0$.

(3) $\langle \chi, \chi \rangle = 1$ *si y sólo si χ es irreducible.*

Demostración. La parte 1 se sigue del teorema 14.4 de ortogonalidad de los caracteres irreducibles. La parte 2 es consecuencia de (1), y para la parte 3 observe que $\langle \chi, \chi \rangle = \sum_{i=1}^{r} m_i^2 = 1$ si y sólo si uno de los $m_i = 1$ y los otros son cero, i.e., si y sólo si $V \simeq W_i$. □

COROLARIO 14.8. *Toda representación irreducible ρ_i de un grupo finito G está contenida en la representación regular de G, con multiplicidad m_i igual al grado n_i de ρ_i.*

Demostración. Por el ejemplo 2, el carácter χ_R de la representación regular de G está dado por

$$\chi_R(g) = \begin{cases} 0 & \text{si } g \neq 1, \\ |G| & \text{si } g = 1. \end{cases}$$

Ahora, por el corolario 14.5 la multiplicidad m_i con que la representación irreducible W_i, con carácter χ_i, está contenida en la representación regular R de G es

$$m_i = \langle \chi_R, \chi_i \rangle = \frac{1}{|G|} \sum_{g \in G} \chi_R(g^{-1})\chi_i(g) = \frac{1}{|G|}\chi_R(1)\chi_i(1) = \frac{1}{|G|}|G|\chi_i(1) = n_i$$

ya que $\chi_i(1) = n_i$ es el grado de la representación irreducible W_i. □

COROLARIO 14.9. (1) *Si G es un grupo finito, entonces tiene sólo un número finito de representaciones irreducibles no isomorfas, con caracteres $\chi_1, \ldots, \chi_r$.*

(2) *Los grados* n_i *de los de los caracteres irreducibles* χ_i *de* G *satisfacen* $\sum_{i=1}^{r} n_i^2 = |G|$.

(3) *Si* $g \in G$, $g \neq 1$, *entonces* $\sum_{i=1}^{r} n_i \chi_i(g) = 0$.

Demostración. (1): Por el corolario anterior todas las representaciones irreducibles de G están contenidas en la representación regular V_R cuyo grado es $|G|$, y como V_R sólo tiene un número finito de subespacios no isomorfos, entonces la parte 1 se sigue.
(2): Por el corolario anterior

$$(*) \qquad \chi_R(g) = \sum_{i=1}^{r} n_i \chi_i(g)$$

para todo $g \in G$. Poniendo $g = 1$ obtenemos

$$|G| = \chi_R(1) = \sum_{i=1}^{r} n_i \chi_i(1) = \sum_{i=1}^{r} n_i n_i = \sum_{i=1}^{r} n_i^2,$$

lo cual prueba (2). Poniendo $g \neq 1$ en $(*)$ se obtiene

$$\sum_{i=1}^{r} n_i \chi_i(g) = \chi_R(g) = 0$$

donde la última igualdad es porque $\chi_R(g)$ es el carácter de la representación regular y $g \neq 1$. □

Observación. La parte 2 del corolario anterior nos da un criterio para la búsqueda de los caracteres irreducibles de un grupo G: supongamos que por algún medio ya encontramos que $\chi_1, \ldots, \chi_r$ son caracteres irreducibles de G, de grados $n_1, \ldots, n_r$. Entonces, éstos son todos si y sólo si $\sum n_i^2 = |G|$.

Ejemplo 6. Para el grupo cíclico $\mathbb{Z}/n\mathbb{Z}$, en el ejemplo 3 del capítulo 13 obtuvimos n representaciones irreducibles de grado 1, $\rho_\omega : \mathbb{Z}/n\mathbb{Z} \to \mathbb{C}^*$, para $\omega \in \mu_n$, y cuyos caracteres calculamos en el ejemplo 4 de este capítulo, como $\chi_\omega(j) = \omega^j$, para $0 \leq j < n$, y como $n = |\mathbb{Z}/n\mathbb{Z}|$, entonces

$$n = |\mathbb{Z}/n\mathbb{Z}| = \sum_{i=1}^{n} n_i^2 = \sum_{i=1}^{n} 1,$$

entonces éstos son todos los caracteres irreducibles del grupo cíclico $\mathbb{Z}/n\mathbb{Z}$.

Ejemplo 7. Si G es un grupo abeliano finito de orden n, en el ejemplo 13 del capítulo 13 construimos n representaciones irreducibles de grado 1 de G, por lo que la parte 2 del corolario anterior se cumple y así éstas son todas las representaciones irreducibles

de G. Note que en el ejemplo 16 del capítulo 13 y en el corolario 13.6, mostramos que todas las representaciones irreducibles de G son de grado 1.

El teorema siguiente nos dice exactamente cuántas representaciones irreducibles tiene un grupo finito G en términos de la estructura del grupo. Antes necesitaremos unas definiciones y un lema:

Funciones de clases. Si $\chi : G \to \mathbb{C}$ es un carácter de G, por 14.1(2) sabemos que $\chi(tgt^{-1}) = \chi(g)$, para cualesquiera $g, t \in G$ y ésto nos dice que todo carácter χ es constante en cada clase de conjugación de G. En general, una función $f : G \to \mathbb{C}$ que es constante en cada clase de conjugación de G, i.e., tal que $f(tgt^{-1}) = f(g)$, para todo $g, t \in G$, se llamará una *función de clases*. Sea $\mathcal{F}$ el conjunto de todas las funciones de clases en G. Es claro que la suma de dos funciones de clases es una función de clases y que el producto de un escalar por una función de clases también es una función de clases. Como la función constante cero $0 : G \to \mathbb{C}$ está en $\mathcal{F}$, se sigue que $\mathcal{F}$ es un $\mathbb{C}$-subespacio vectorial del espacio de todas las funciones de G en $\mathbb{C}$ y por lo tanto podemos considerar el producto escalar

$$\langle f, h\rangle := \frac{1}{|G|}\sum_{\sigma\in G} f(\sigma^{-1}h(\sigma),$$

definido anteriormente, restringido a $\mathcal{F}$. Por 14.4 los caracteres irreducibles $\chi_1, \ldots, \chi_r$ de G forman un sistema ortonormal en $\mathcal{F}$, y son un conjunto finito por 14.9. Mostraremos que forman una base y para ésto necesitaremos el lema siguiente:

LEMA 14.10. *Sean $f : G \to \mathbb{C}$ una función de clases y $\rho : G \to \mathrm{GL}(V)$ una representación. Sea $\rho_f : V \to V$ la función lineal dada por*

$$\rho_f := \sum_{\sigma\in G} f(\sigma)\rho(\sigma).$$

Si ρ es irreducible de grado n y carácter χ, entonces ρ_f es una homotecia de razón λ dada por

$$\lambda := \frac{1}{n}\sum_{\sigma\in G} f(\sigma)\chi(\sigma) = \frac{|G|}{n}\langle f, \overline{\chi}\rangle.$$

Demostración. Mostraremos que ρ_f satisface la condición del lema de Schur. En efecto, para todo $t \in G$:

$$\rho(t^{-1})\rho_f\rho(t) = \sum_{\sigma\in G} \rho(t)^{-1}f(\sigma)\rho(\sigma)\rho(t) = \sum_{\sigma\in G} f(\sigma)\rho(t^{-1}\sigma t)$$

(la última igualdad por linealidad, ya que $f(\sigma) \in \mathbb{C}$), y poniendo $u := t^{-1}\sigma t$, i.e., $\sigma = tut^{-1}$, y usando que f es función de clases, la igualdad anterior se vuelve

$$\rho(t)^{-1}\rho_f\rho(t) = \sum_{u\in G} f(tut^{-1})\rho(u) = \sum_{u\in G} f(u)\rho(u) = \rho_f.$$

es decir, $\rho_f \rho(t) = \rho(t)\rho_f$, y así, por la parte 2 del lema de Schur, se tiene que ρ_f es una homotecia, $\rho_f = \lambda \, \mathrm{id}_V$. Calculando trazas en esta igualdad:

$$n\lambda = \mathrm{Tr}(\lambda \, \mathrm{id}_V) = \mathrm{Tr}(\rho_f) = \sum_{\sigma \in G} f(\sigma)\mathrm{Tr}(\rho(\sigma)) = \sum_{\sigma \in G} f(\sigma)\chi(\sigma)$$

y así

$$\lambda = \frac{1}{n} \sum_{\sigma \in G} f(\sigma)\chi(\sigma) = \frac{1}{n}|G|\langle f, \overline{\chi}\rangle,$$

la última igualdad por la definición del producto interno. □

El resultado principal es:

TEOREMA 14.11. *Sea G un grupo finito. Entonces,*

(1) *Los caracteres irreducibles $\chi_1, \ldots, \chi_r$ de G forman una base del espacio de funciones de clases $\mathcal{F}$.*

(2) *El número de representaciones irreducibles de G, salvo isomorfismo, es igual al número de clases de conjugación de G.*

Demostración. Por 14.4 los caracteres irreducibles $\chi_1, \ldots, \chi_r$ de G forman un sistema ortonormal en $\mathcal{F}$ y por lo tanto son linealmente independientes. Para mostrar que generan $\mathcal{F}$ es suficiente mostrar que todo elemento de $\mathcal{F}$ ortogonal a todos los $\overline{\chi}_i$ es cero. Sea $f \in \mathcal{F}$ un tal elemento, i.e., $\langle f, \overline{\chi}_i\rangle = 0$, para todo i. Para cada representación ρ de G pongamos $\rho_f := \sum \sigma \in G f(\sigma)\rho(\sigma)$ como en el lema. Si ρ es irreducible, su carácter χ es uno de los χ_i y por el lema anterior se sigue que ρ_f es (la homotecia) cero ya que $\langle f, \overline{\chi}\rangle = \langle f, \overline{\chi}_i\rangle = 0$, por la suposición que hicimos sobre f. Si ρ no fuera irreducible, descomponiéndolo en suma directa de irreducibles ρ_j se sigue también que $\rho_f = 0$.

Apliquemos lo anterior a la representación regular $R : G \to \mathrm{GL}(V)$, donde el espacio vectorial V tiene como base a $\mathcal{B} = \{v_g\}_{g \in G}$. Ahora, para el básico $v_1 \in \mathcal{B}$, i.e., con $g = 1$, calculemos su imagen bajo la función lineal $R_f : V \to V$ asociada a R como en el lema previo. Entonces

$$(\dagger) \qquad R_f v_1 = \Big(\sum_{\sigma \in G} f(\sigma)R(\sigma)\Big)v_1 = \sum_{\sigma \in G} f(\sigma)R(\sigma)(v_1) = \sum_{\sigma \in G} f(\sigma)v_\sigma$$

(ya que $R(\sigma)(v_g) = v_{\sigma g}$). Ahora, por la primera parte de esta demostración, $R_f = 0$ y así $R_f(v_1) = 0$, por lo que la igualdad (†) implica que los coeficientes $f(\sigma) = 0$ para todo $\sigma \in G$ ya que los v_σ son linealmente independientes. Se sigue que $f = 0$, lo cual prueba (1).

Para (2), sean $C_1, \ldots, C_k$ las clases de conjugación de G. Si $f : G \to \mathbb{C}$ es una función de clases, entonces f es constante en cada clase C_i y los valores (constantes) $\lambda_i \in \mathbb{C}$ de f en cada C_i pueden ser elegidos arbitrariamente. Por lo tanto, escogiendo

$\lambda_i = 1$ se tienen k funciones $f_i : G \to \mathbb{C}$ dadas por $f_i(C_j) = \delta_{ij}$, y si $f : G \to \mathbb{C}$ es cualquier función de clases con valores $f(C_i) = \lambda_i$, entonces $f = \sum \lambda_i f_i$, y así las f_i generan a $\mathcal{F}$ y es obvio que son linealmente independientes, por lo que $\dim_{\mathbb{C}}(\mathcal{F}) = k$ (el número de clases de conjugación de G). Pero por la parte 1, $\dim_{\mathbb{C}}(\mathcal{F}) = r$ (el número de caracteres irreducibles de G), y así $k = r$, como se quería. □

COROLARIO 14.12. *Sea G un grupo finito y sean $\chi_1, \ldots, \chi_r$ los caracteres irreducibles de G. Entonces,*

$$\sum_{i=1}^{r} \overline{\chi_i}(\sigma)\chi_i(t) = \begin{cases} |G|/|C_\sigma| & \text{si } t \in C_\sigma \text{ (la clase de conjugación de } \sigma), \\ 0 & \text{si } t \notin C_\sigma. \end{cases}$$

Demostración. Sea $f_\sigma : G \to \mathbb{C}$ la función que es 1 en C_σ y cero en las otras clases. Por la proposición anterior $f_\sigma = \sum_{i=1}^{r} \lambda_i \chi_i$, donde

$$\lambda_i = \langle f_\sigma, \chi_i \rangle = \frac{1}{|G|} \sum_{g \in G} f_\sigma(g)\overline{\chi_i}(g) = \frac{1}{|G|} \sum_{g \in C_\sigma} \overline{\chi_i}(g) = \frac{|C_\sigma|}{|G|}\overline{\chi_i}(\sigma)$$

y así, para cada $t \in G$,

$$f_\sigma(t) = \frac{|C_\sigma|}{|G|} \sum_{i=1}^{r} \overline{\chi_i}(\sigma)\chi_i(t)$$

lo cual da el resultado deseado poniendo primero $t \in C_\sigma$ y luego $t \notin C_\sigma$. □

La tabla de caracteres de un grupo finito. Si G es un grupo finito, por 14.11 el número de representaciones irreducibles de G es igual al número de clases de conjugación de G. Sean $\rho_1, \ldots, \rho_r$ estas representaciones irreducibles y sean $\chi_1, \ldots, \chi_r$ los caracteres irreducibles asociados. Por convención ρ_1 es la representación trivial y χ_1 es el carácter principal asociado.

Como cada carácter (irreducible) χ_i queda especificado por sus valores en un representante de cada clase de conjugación de G, entonces los r caracteres irreducibles χ_i están determinados por una tabla cuadrada $r \times r$ cuyas entradas son los valores de los r caracteres χ_i en los r representantes g_j de las r clases de conjugación C_j de G. Este arreglo $r \times r$ se llama la *tabla de caracteres* del grupo G, que, por supuesto, sólo está bien definida salvo el orden de sus renglones o columnas. Al escoger un orden en las clases de conjugación, por convención elegimos $g_1 = 1$ de tal forma que $C_1 = \{1\}$. En la tabla de caracteres pondremos en el renglón superior a los representantes de las clases de conjugación $1 = g_1, g_2, \ldots, g_r$, y en la columna de la izquierda a los caracteres $\chi_1, \ldots, \chi_r$, con χ_1 el carácter principal de G. Es usual también poner arriba de cada representante g_i al orden h_i de su clase de conjugación C_i. Note que como $g_1 = 1$, entonces $h_1 = 1$ y también observamos que $\chi_i(1) = n_i$ es el grado del carácter χ_i. Esto determina la primera columna de la tabla. También, como χ_1 es el carácter principal de G y éste es irreducible, entonces es igual al carácter trivial, por lo

que $\chi_1(g_i) = 1$ para todo g_i. Esto determina el primer renglón de la tabla. Recuerde que $h_i = |C_{g_i}| = [G : C_G(g_i)]$.

$h_i =$	1	h_2	h_3	$\cdots$	h_r
$g_i =$	1	g_2	g_3	$\cdots$	g_r
χ_1	1	1	1	$\cdots$	1
χ_2	n_2	$\chi_2(g_2)$	$\chi_2(g_3)$	$\cdots$	$\chi_2(g_r)$
$\vdots$					
χ_r	n_r	$\chi_r(g_2)$	$\chi_r(g_3)$	$\cdots$	$\chi_r(g_r)$

Ahora, los renglones de esta tabla los podemos ver como vectores en $\mathbb{C}^r$ con el carácter χ_i fijo y variando los representantes g_i de las clases de conjugación:

$$(\chi_i(1), \chi_i(g_2), \chi_i(g_3), \ldots, \chi_i(g_r))$$

y el teorema de ortogonalidad 14.4 nos dice que estos renglones son ortonormales. Lo enunciamos para renombrarlo:

TEOREMA 14.13 (Ortogonalidad por renglones). *Si G es un grupo finito y $\chi_1, \ldots, \chi_r$ son sus caracteres irreducibles, entonces*

$$\langle \chi_i, \chi_j \rangle = \delta_{ij},$$

lo cual, por definición del producto interno, se puede escribir como

$$\delta_{ij} = \frac{1}{|G|} \sum_{\sigma \in G} \chi_i(\sigma)\overline{\chi}_j(\sigma) = \frac{1}{|G|} \sum_{t=1}^{r} h_t \chi_i(g_t)\overline{\chi}_j g_t)$$

donde $h_t = |C_t|$ y $g_t \in C_t$, para C_t las clases de conjugación de G.

□

Ahora, fijándonos en las columnas de la tabla los pensamos como vectores en $\mathbb{C}^r$ con el representante g_j de la clase de conjugación fijo y variando los caracteres χ_i:

$$\begin{pmatrix} \chi_1(g_j) \\ \chi_2(g_j) \\ \vdots \\ \chi_r(g_j) \end{pmatrix}$$

y el corolario 14.12 se lee ahora como:

TEOREMA 14.14 (Ortogonalidad por columnas). *Si G es un grupo finito y $\chi_1, \ldots, \chi_r$ son sus caracteres irreducibles, g_j son representantes de sus clases de conjugación y h_j son los órdenes de estas clases, entonces*

$$\sum_{t=1}^{r} \chi_t(g_i)\overline{\chi}_t(g_j) = \frac{|G|}{h_i}\delta_{ij} = |C_G(g_i)|\delta_{ij}$$

donde la última igualdad es por el teorema órbita-estabilizador y el ejemplo 12 del capítulo 8. □

En ocasiones las relaciones de ortogonalidad ayudan a completar la tabla de caracteres de un grupo, como veremos en los ejemplos siguientes:

Ejemplo 8. Sea $G = A_4$, el grupo alternante en 4 letras. Las clases de conjugación de A_4 son:

$$C_1 = \{1\}$$
$$C_2 = \{(12)(34),\ (13)(24),\ (14)(23)\}$$
$$C_3 = \{(123),\ (142),\ (134),\ (243)\}$$
$$C_4 = \{(132),\ (124),\ (143),\ (234)\}$$

y así A_4 tiene 4 caracteres irreducibles. Ahora, del ejercicio 14 del capítulo 5, el subgrupo conmutador de A_4 es

$$[A_4, A_4] = \{1,\ (12)(34),\ (13)(24),\ (14)(23)\}$$

y así tiene índice 3 en A_4, por lo que $A_3/[A_4, A_4] \simeq \mathbb{Z}/3\mathbb{Z}$ y consecuentemente A_4 tiene 3 caracteres irreducibles de grado 1, por el ejercicio 5 del capítulo 13, las cuales se obtienen de los 3 caracteres de grado 1 del grupo cíclico $\mathbb{Z}/3\mathbb{Z}$ que, por el ejemplo 5 están dadas, eligiendo una raíz cúbica $\omega \in \mu_3$, mediante $\chi_\omega(j) = \omega^j$ para $j \in \mathbb{Z}/3\mathbb{Z}$: Para $\omega = 1$, χ_1 es el carácter principal. Para $\omega = \exp(2\pi i/3)$, el carácter χ_2 correspondiente está dado como sigue: como en el cociente $A_4/[A_4, A_4] \simeq \mathbb{Z}/3\mathbb{Z}$ se tiene que $[A_4, A_4] = C_1 \cup C_2$, entonces los elementos de estas clases representan al $0 \in \mathbb{Z}/3\mathbb{Z}$, por lo que si $\sigma \in C_1 \cup C_2$, entonces $\chi_2(\sigma)$ está dado por $\sigma \mapsto 0 \mapsto \omega^0 = 1$ y así $\chi_2(\sigma) = 1$ para $\sigma \in C_1 \cup C_2$. Ahora, si $\sigma \in C_3$, por ejemplo si $\sigma = (123)$, entonces σ es de orden 3 y así, representa al 1 en el cociente $A_4/[A_4, A_4] \simeq \mathbb{Z}/3\mathbb{Z}$. Se sigue que $\chi_2(\sigma) = \omega^1 = \omega$, para toda $\sigma \in C_3$. Finalmente, si $\sigma \in C_4$, no le queda más que representar al 2 en el cociente $A_4/[A_4, A_4] \simeq \mathbb{Z}/3\mathbb{Z}$, por lo que $\chi_2(\sigma) = \omega^2$ para todo $\sigma \in C_4$. Se sigue que χ_2 está dado por

$$\chi_2(\sigma) = \begin{cases} 1 & \text{si } \sigma \in C_1 \cup C_2, \\ \omega & \text{si } \sigma \in C_3, \\ \omega^2 & \text{si } \sigma \in C_4. \end{cases}$$

Similarmente, para la tercera raíz cúbica ω^2, el carácter χ_3 correspondiente estado por

$$\chi_3(\sigma) = \begin{cases} 1 & \text{si } \sigma \in C_1 \cup C_2, \\ \omega^2 & \text{si } \sigma \in C_3, \\ \omega & \text{si } \sigma \in C_4. \end{cases}$$

Sólo falta encontrar el cuarto carácter irreducible χ_4 de A_4. Ahora, como $|A_4| = 12$, por el corolario 14.9 si n_4 es su grado, se debe tener que

$$12 = 1^2 + 1^2 + 1^2 + n_4^2$$

y así $n_4 = 3$, i.e., χ_4 es un carácter de grado 3. Por lo tanto, como $\chi_4(1) = n_4 = 3$, sólo nos falta calcular $\chi_4(\sigma)$ para $\sigma \in C_i$ con $i = 2, 3, 4$. Para ésto, usaremos las relaciones de ortogonalidad $\langle \chi_i, \chi_4 \rangle = 0$ para $i = 1, 2, 3$. Pongamos

$$\chi_4(\sigma) = \begin{cases} a & \text{si } \sigma \in C_2, \\ b & \text{si } \sigma \in C_3, \\ c & \text{si } \sigma \in C_4. \end{cases}$$

Entonces, por definición del producto interior y porque $|C_1| = 1$, $|C_2| = 3$, $|C_3| = |C_4| = 4$, se tiene que

$$0 = \langle \chi_1, \chi_4 \rangle = \frac{1}{12}(1 \cdot 3 + 3 \cdot 1 \cdot a + 4 \cdot 1 \cdot b + 4 \cdot 1 \cdot c) = \frac{1}{12}(3 + 3a + 4b + 4c)$$

$$0 = \langle \chi_2, \chi_4 \rangle = \frac{1}{12}(3 + 3a + 4\omega^2 b + 4\omega c)$$

$$0 = \langle \chi_3, \chi_4 \rangle = \frac{1}{12}(3 + 3a + 4\omega b + 4\omega^2 c)$$

y resolviendo este sistema de ecuaciones en a, b, c se obtiene que $a = -1$ y $b = 0 = c$, por lo que

$$\chi_4(\sigma) = \begin{cases} 3 & \text{si } \sigma \in C_1 = \{1\}, \\ -1 & \text{si } \sigma \in C_2, \\ 0 & \text{si } \sigma \in C_3 \cup C_4. \end{cases}$$

Así, la tabla de caracteres de A_4 es:

$h_i =$	1	3	4	4
$g_i =$	1	(12)(34)	(123)	(132)
χ_1	1	1	1	1
χ_2	1	1	ω	ω^2
χ_3	1	1	ω^2	ω
χ_4	3	-1	0	0

con $\omega = \exp(2\pi i/3)$.

Ejemplo 9. Sea S_3 el grupo simétrico en 3 letras. Recordemos, del capítulo 4, que las clases de conjugación de S_n consisten de todas las permutaciones que tienen la misma estructura cíclica (4.12). Se sigue que las clases de conjugación de S_3 son

$$C_1 = \{1\},\ C_2 = \{(12),\ (13),\ (23)\},\ C_3 = \{(123),\ (132)\}$$

por lo que S_3 tiene 3 caracteres irreducibles. Ahora, como $S_3/A_3 \simeq \mathbb{Z}/2\mathbb{Z}$, entonces S_3 tiene 2 caracteres χ_1 y χ_2 de grado 1, que son el carácter principal χ_1 y el carácter de la función signo (ejemplo 4 del capítulo 13). Así, $\chi_2(1) = \operatorname{sgn}(1) = 1$, $\chi_2(1,2) = \operatorname{sgn}(1,2) = -1$ y $\chi_2(1,2,3) = \operatorname{sgn}(1,2,3) = 1$, por lo que la tabla de caracteres de S_3 empieza como:

$h_i =$	1	3	2
$g_i =$	1	(12)	(123)
χ_1	1	1	1
χ_2	1	-1	1
χ_3			

Para calcular el grado n_3 de χ_3 , como

$$6 = |S_3| = n_1^2 + n_2^2 + n_3^2 = 1 + 1 + n_3^2 = 2 + n_3^2,$$

entonces $n_3 = 2$ y así $\chi_3(1) = 2$, lo cual agregamos a la primera columna. Ahora, para calcular el lugar faltante en la segunda columna, observemos que la ortogonalidad por columnas implica:

$$0 = \sum_{i=1}^{3} n_i\chi_i(12) = 1\cdot\chi_1(12) + 1\cdot\chi_2(12) + 2\cdot\chi_3(12) = 1\cdot 1 + 1\cdot(-1) + 2\cdot\chi_3(12)$$

por lo que $2\chi_3(12) = 0$, i.e., $\chi_2(12) = 0$. Similarmente, para el lugar faltante en la tercera columna,

$$0 = \sum_{i=1}^{3} n_i\chi_i(123) = 1\cdot\chi_1(123) + 1\cdot\chi_2(123) + 2\cdot\chi_3(123) = 1\cdot 1 + 1\cdot 1 + 2\cdot\chi_3(12)$$

por lo que $\chi_3(123) = -1$. Podemos entonces completar la tabla de caracteres de S_3:

$h_i =$	1	3	2
$g_i =$	1	(12)	(123)
χ_1	1	1	1
χ_2	1	-1	1
χ_3	2	0	-1

Ejemplo 10. Sea $\langle\sigma\rangle \simeq \mathbb{Z}/n\mathbb{Z}$ un grupo cíclico finito de orden n. Si $\omega = \exp(2\pi i/n)$ es una raíz primitiva n-ésima de la unidad, por el ejemplo 3 los n caracteres irreducibles de $\mathbb{Z}/n\mathbb{Z}$ (hay n clases de conjugación porque es abeliano) son de grado 1 y están dados por

$$\chi_i(\sigma) := \omega^{i-1}, \quad 1 \leq i \leq n,$$

i.e., $\chi_i(\sigma^k) = \omega^{k(i-1)}$, para $k \in \mathbb{Z}/n\mathbb{Z}$. La tabla de caracteres de $\mathbb{Z}/n\mathbb{Z} \simeq \langle\sigma\rangle$ es:

$h_i =$	1	1	1	$\cdots$	1
$g_i =$	1	σ	σ^2	$\cdots$	σ^{n-1}
χ_1	1	1	1	$\cdots$	1
χ_2	1	ω	ω^2	$\cdots$	$\omega^{(n-1)}$
χ_3	1	ω^2	ω^4	$\cdots$	$\omega^{2(n-2)}$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\cdots$	$\vdots$
χ_n	1	ω^{n-1}	$\omega^{2(n-1)}$	$\cdots$	$\omega^{(n-1)(n-1)}$

Ejemplo 11. Sea G cualquier grupo abeliano finito. Como G es abeliano sus clases de conjugación tienen un único elemento y así, por 14.11, G tiene $|G|$ caracteres irreducibles χ_i. Ahora, por el corolario 14.9, $|G| = \sum_{i=1}^{|G|} n_i^2$, donde n_i es el grado de χ_i. Esta igualdad implica que todos los $n_i = 1$, por lo que todos los caracteres irreducibles de G son de grado 1. En el ejemplo 13 del capítulo 13 construimos $|G|$ representaciones irreducibles de grado 1 de G, necesariamente irreducibles. La afirmación recíproca también es válida: si todas las representaciones irreducibles de un grupo G son de grado 1, entonces G es abeliano. En efecto, el número r de representaciones irreducibles de G es igual al número de clases de conjugación de G y se tiene que $|G| = \sum_{i=1}^{|G|} n_i^2$, donde cada $n_i = 1$ por lo que $|G| = r$ y así G tiene $|G|$ clases de conjugación por lo que cada una de éstas debe contener un único elemento y por lo tanto G es abeliano. Una consecuencia inmediata de este ejemplo es:

COROLARIO 14.15. *Si G es un grupo finito de orden n y H es un subgrupo abeliano de G, entonces el grado de cada representación irreducible de G es $\leq [G : H]$*

Demostración. Sea $\rho : G \to \mathrm{GL}(V)$ una representación irreducible de G. Restringiendo ρ a H se obtiene una representación $\rho_H : H \to \mathrm{GL}(V)$ de H. Sea $W \subseteq V$ una subrepresentación irreducible de ρ_H. Como H es abeliano, por el ejemplo anterior $\dim W = 1$. Sea $V' \subseteq V$ el subespacio vectorial generado por las imágenes $\rho(\sigma)W$, con σ recorriendo G. Es claro que V' es G-invariante y como V es irreducible, entonces $V' = V$. Ahora, para $g \in G$ y $h \in H$ se tiene que

$$\rho(gh)W = \rho(g)\rho(h)W = \rho(g)W$$

ya que $\rho(h)W = W$ porque $\rho(h) : W \to W$ es isomorfismo. Así, para todo $gh \in gH$ se tiene que $\rho(gh)W = \rho(g)W$ por lo que el número de $\rho(g)W$ distintas es a lo más $[G : H]$, y como $V = V'$ es la suma de los $\rho(g)W$, con cada $\rho(g)W$ de dimensión 1, y por lo que acabamos de ver hay a lo más $[G : H]$ distintas $\rho(g)W$, entonces $\dim V \leq [G : H]$. □

Ejemplo 12. Para el grupo diédrico D_{2n}, sabemos, por el ejercicio 9 del capítulo 5, que contiene al grupo R_n de rotaciones y que $[D_{2n} : R_n] = 2$. Por el corolario anterior las representaciones irreducibles de D_{2n} son de grado 1 ó 2. Ahora, D_{2n} tiene como generadores a la rotación $r = r_{2\pi/n}$ y a la reflexión ρ, y estos generadores satisfacen las relaciones

$$r^n = 1,\ \rho^2 = 1,\ \rho r \rho = r^{-1}.$$

Además, cada elemento $g \in D_{2n}$ se puede escribir, en forma única, como

$$g = \begin{cases} r^k & \text{con } 0 \leq k \leq n-1 \quad \text{si } g \in R_n, \\ \rho r^k & \text{con } 0 \leq k \leq n-1 \quad \text{si } g \notin R_n, \text{ i.e., si } g \text{ es una reflexión.} \end{cases}$$

Observe que $\rho r \rho = r^{-1}$ implica que $\rho r^k \rho = (\rho r \rho)^k = \rho^{-k}$ y por lo tanto $\rho r^k \rho r^k = 1$, i.e., $(\rho r^k)^2 = 1$, por lo que los elementos de la forma ρr^k son reflexiones.

Para calcular las representaciones irreducibles de D_{2n}, ya sabemos que éstas son de grados 1 ó 2. Ahora, si $\phi : D_{2n} \to \mathrm{GL}(V) \simeq \mathrm{GL}(2, \mathbb{C})$ es una representación de grado 2, diagonalizando la matriz $\phi(g)$, con $g \in D_{2n}$, note que si $g = r \in R_n$, como $r^n = 1$, se tiene que

$$I_2 = [\phi(r)]^n = \begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix}^n = \begin{pmatrix} \lambda_1^n & 0 \\ 0 & \lambda_2^n \end{pmatrix}$$

por lo que λ_1 y λ_2 son raíces n-ésimas de la unidad. Esto nos motiva a definir, para $\omega \in \mu_n$ una raíz n-ésima de la unidad, la función

$$\phi_\omega : D_{2n} \to \mathrm{GL}(2, \mathbb{C})$$

mediante

$$\phi_\omega(r^k) := \begin{pmatrix} \omega^k & 0 \\ 0 & \omega^{-k} \end{pmatrix} \quad \text{y} \quad \phi_\omega(\rho r^k) := \begin{pmatrix} 0 & \omega^{-k} \\ \omega^k & 0 \end{pmatrix}.$$

Es inmediato verificar que ϕ_ω es un homomorfismo y así tenemos n representaciones de D_{2n} de grado 2, una por cada raíz de la unidad $\omega \in \mu_n$. La pregunta natural, en este contexto, es: ¿cuándo es ϕ_ω reducible? Para que ϕ_ω sea reducible debe existir un subespacio $W \subseteq \mathbb{C}^2$ de dimensión 1 y que sea D_{2n}-invariante. Sea $v = (x, y) \in \mathbb{C}^2$ tal que $W = \langle v \rangle$ es D_{2n}-invariante. Entonces, para todo $g \in D_{2n}$ debe existir un $\lambda \in \mathbb{C}^*$ tal que

$$(*) \qquad \phi_\omega(g)v = \lambda v$$

y ésto basta considerarlo en los generadores $g = r$ y ρ de D_{2n}, i.e., para

$$\phi_\omega(r) := \begin{pmatrix} \omega & 0 \\ 0 & \omega^{-1} \end{pmatrix} \quad \text{y} \quad \phi_\omega(\rho) := \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

por lo que $(*)$ se vuelve

$$\phi_\omega(r)v := \begin{pmatrix} \omega & 0 \\ 0 & \omega^{-1} \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} \omega x \\ \omega^{-1} y \end{pmatrix} = \lambda \begin{pmatrix} x \\ y \end{pmatrix}$$

y

$$\phi_\omega(\rho)v := \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} y \\ x \end{pmatrix} = \lambda' \begin{pmatrix} x \\ y \end{pmatrix}$$

que dan lugar al sistema de ecuaciones:

$$\begin{aligned} \omega x &= \lambda x \\ \omega^{-1} y &= \lambda y \\ y &= \lambda' x \\ x &= \lambda' y. \end{aligned}$$

Donde observamos que, como $\lambda' \neq 0$, de las dos últimas ecuaciones se deduce que $x = y = 0$ ó $x \neq 0$ y $y \neq 0$. Ahora, como $v = (x, y)$ es generador de W, que tiene dimensión 1, entonces $v \neq 0$, por lo que $x \neq 0$ ó $y \neq 0$, que combinado con las condiciones anteriores nos dice que $x \neq 0$ y $y \neq 0$. Así, de las dos primeras ecuaciones se sigue que $\lambda = \omega = \omega^{-1}$, i.e., $\omega^2 = 1$, i.e., $\omega \in \mu_2$ y por lo tanto

$$\phi_\omega \text{ es reducible } \Leftrightarrow \omega \in \mu_2 \subseteq \mu_n.$$

De hecho, notamos que si $\omega \in \mu_2$ y si $v_1 = (1, 1)$ y $v_2 = (1, -1)$, los subespacios

$$W_1 = \langle v_1 \rangle \quad \text{y} \quad W_2 = \langle v_2 \rangle$$

son D_{2n}-invariantes y $W_1 \oplus W_2 = \mathbb{C}^2$.

Ahora, para $\omega = 1$ y para la representación $\phi_1 : D_{2n} \to \mathrm{GL}(2, \mathbb{C})$, calculando $\phi_1(r)$ y $\phi_1(\rho)$ en la base $\{v_1, v_2\}$ de $\mathbb{C}^2$:

$$\phi_1(r) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad \text{y} \quad \phi_1(\rho) = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

que dan lugar a las subrepresentaciones de grado 1:

$$T_1 : D_{2n} \to \mathrm{GL}(1, \mathbb{C}) \quad \text{dada por } T_1(r) = 1 \text{ y } T_1(\rho) = 1$$

y

$$T_2 : D_{2n} \to \mathrm{GL}(1, \mathbb{C}) \quad \text{dada por } T_2(r) = 1 \text{ y } T_2(\rho) = -1$$

que satisfacen $T_1 \oplus T_2 = \phi_1$.

Distinguimos ahora dos casos, dependiendo de la paridad del entero n en D_{2n}:

CASO 1. Si n es *par*. En este caso $-1 \in \mu_n$ y como $-1 \in \mu_2$, para la representación $\phi_{-1} : D_{2n} \to \mathrm{GL}(2, \mathbb{C})$, en la base $\{v_1, v_2\}$ se tiene que

$$\phi_{-1}(r) = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \quad \text{y} \quad \phi_{-1}(\rho) = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$$

que dan lugar a las subrepresentaciones de grado 1:

$$T_3 : D_{2n} \to \mathrm{GL}(1, \mathbb{C}) \quad \text{dada por } T_3(r) = -1 \text{ y } T_3(\rho) = -1$$

y

$$T_4 : D_{2n} \to \mathrm{GL}(1, \mathbb{C}) \quad \text{dada por } T_4(r) = -1 \text{ y } T_4(\rho) = 1$$

que satisfacen $T_3 \oplus T_4 = \phi_{-1}$.

Así, si n es par hemos construido 4 representaciones de grado 1 que son subrepresentaciones correspondientes a las representaciones ϕ_1 y ϕ_{-1} asociadas a las dos raíces $1, -1 \in \mu_2 \subseteq \mu_n$ que son las únicas representaciones de grado 2 reducibles de D_{2n}. Se sigue que, si $\omega \in \mu_n - \mu_2$, la representación ϕ_ω correspondiente es irreducible. Observe ahora que como $\omega^k \omega^{n-k} = 1$, entonces ϕ_{ω^k} y $\phi_{\omega^{n-k}}$ son isomorfas. Se sigue que sólo necesitamos considerar las representaciones de grado 2 asociadas a las raíces ω^k con $0 \leq k \leq n/2$ (recuerde que n es par) y observamos que los casos $k = 0$ y $k = n/2$ corresponden a las raíces 1 y -1, que ya vimos que son reducibles. Nos hemos quedado así con $(n/2) - 1$ representaciones irreducibles de grado 2. Mostraremos ahora que éstas no son isomorfas entre sí. En efecto, si $\omega, \omega' \in \mu_n$, entonces ϕ_ω es isomorfa a $\phi_{\omega'}$ si y sólo si $\chi_{\phi_\omega} = \chi_{\rho_{\omega'}}$, por 14.6. Pero, por definición de ϕ_ω y $\phi_{\omega'}$,

$$\chi_{\phi_\omega} = 2\mathrm{Re}\,(\omega^k) = \chi_{\rho_{\omega'}} = 2\mathrm{Re}\,(\omega'^k), \quad 0 \leq k < n$$

en particular $\mathrm{Re}\,(\omega) = \mathrm{Re}\,(\omega')$, y como $\omega, \omega' \in \mu_n$, esto sucede si y sólo si $\omega = \overline{\omega'}$. Por lo tanto, como los argumentos de ω y ω' son de la forma $2t\pi/n$, con $0 < t < n/2$, entonces $\omega = \overline{\omega'}$ si y sólo si $\omega = \omega'$, y así los ϕ_{ω^k} con $0 < k < n/2$ no son isomorfos. Hemos así probado que: *si n es par, se tienen $(n/2) - 1$ representaciones irreducibles de grado 2 de D_{2n}*. Finalmente, observamos que las 4 representaciones T_i de grado 1 y las $(n/2) - 1$ representaciones irreducibles de grado 2, son todas las representaciones irreducibles de D_{2n} ya que sus grados satisfacen la igualdad

$$4(1^2) + ((n/2) - 1)(2^2) = 4 + 2n - 4 = 2n = |D_{2n}|.$$

CASO 2. Si n es *impar*. En este caso $-1 \notin \mu_n$ y así sólo tenemos dos representaciones T_i de grado 1 correspondientes a subrepresentaciones de ϕ_1. Para las de grado 2, son las mismas que las del caso anterior, con la condición de que $0 < k < n/2$ y sólo observamos que, como n es impar, la condición $k < n/2$ se puede escribir como $k \leq (n-1)/2$, i.e., k debe satisfacer que

$$1 \leq k \leq (n-1)/2.$$

Hemos mostrado así que: *si n es impar, se tienen $(n-1)/2$ representaciones irreducibles de grado 2 de D_{2n}* y junto con las dos representaciones de grado 1 son todas las representaciones irreducibles de D_{2n}, ya que sus grados satisfacen la igualdad

$$2(1^2) + ((n-1)/2)(2^2) = 2 + 2n - 2 = 2n = |D_{2n}|.$$

Los caracteres irreducibles de D_{2n}. Habiendo ya calculado las representaciones irreducibles de D_{2n}, sus caracteres son:

CASO 1. Si n es par. Para las 4 representaciones de grado 1, sus caracteres son ellas mismas: χ_1 (el carácter principal), $\chi_2 = T_2, \chi_3 = T_3, \chi_4 = T_4$. Para los de grado 2,

$$\phi_{\omega^k}(r^t) := \begin{pmatrix} \omega^{kt} & 0 \\ 0 & \omega^{-kt} \end{pmatrix} \quad \text{y} \quad \phi_{\omega^k}(\rho r^t) := \begin{pmatrix} 0 & \omega^{-kt} \\ \omega^{kt} & 0 \end{pmatrix},$$

por lo que sus caracteres son

$$\chi_{\omega^k}(r^t) = \omega^{kt} + \omega^{-kt} = 2\cos\left(\frac{2\pi kt}{n}\right)$$

y

$$\chi_{\omega^k}(\rho r^t) = 0.$$

CASO 2. Si n es impar. Se tienen 2 representaciones de grado 1, cuyos caracteres son ellas mismas. Para los de grado 2, sus caracteres son como los del caso anterior.

Notas. La historia de la matemática no es lineal, y así no debe parecer extraño que la definición de caracteres de grupos precede a la definición del concepto de representación que vimos en el capítulo anterior. En [35] Frobenius definió la noción de carácter de un grupo finito antes de haber llegado al concepto de representación, y en su definición original los caracteres aparecían como soluciones de ciertas ecuaciones y tienen muy poco parecido con la forma en que se definen los caracteres actualmente. Fue en [36] donde Frobenius define la noción de representación de un grupo finito y demuestra que las trazas de las matrices de la representación correspondientes son los caracteres del grupo. La presentación actual de la teoría de representaciones y de caracteres de los grupos finitos, como la hicimos en los capítulos 13 y 14, se debe esencialmente a Schur, alumno doctoral de Frobenius en Berlín, y se encuentra en [52].

EJERCICIO 1. Para las representaciones ρ y ρ' de S_4, dadas en los ejercicios 7 y 8 del capítulo anterior, calcule sus caracteres y responda a la pregunta 9 del capítulo 13.

EJERCICIO 2. Muestre que S_4 tiene exactamente dos representaciones irreducibles de grado 1, dos de grado 3 y una de grado 2. Hallar esta última.

EJERCICIO 3. Calcule la tabla de caracteres de S_4.

EJERCICIO 4. Si $H \lhd G$ y $g \in G$, demuestre que $|C_G(g)| \geq |C_{G/H}(gH)|$.

EJERCICIO 5. Si T es la tabla de caracteres de un grupo finito G, ¿cuál es el determinante de T?

EJERCICIO 6. Si T es la tabla de caracteres de un grupo finito G, demuestre que la suma de las entradas en cada uno de sus renglones es un entero ≥ 0.

EJERCICIO 7. Si $\rho : S_3 \to \mathrm{GL}(3, \mathbb{C})$ es la representación por permutaciones de S_3, vea el ejercicio 10 del capítulo 13, calcule su carácter.

EJERCICIO 8. Sabemos que para todo carácter χ de G, si $g, h \in G$ son conjugados, entonces $\chi(g) = \chi(h)$. Demuestre la afirmación recíproca. *Sugerencia*: suponiendo que $\chi(g) = \chi(h)$ para todo χ, entonces la igualdad es válida para todas las funciones de clases en G, en particular para la función $f : G \to \mathbb{C}$ que es 1 en la clase de conjugación de g y cero fuera.

EJERCICIO 9. Demuestre que g es conjugado de g^{-1} si y sólo $\chi(g)$ es real para todos los caracteres de G.

EJERCICIO 10. Sea χ un carácter de G y sea $g \in G$ de orden 2. Demuestre que $\chi(g)$ es un entero y que $\chi(g) \equiv \chi(1)$ (mód 2).

EJERCICIO 11. Sea χ un carácter de G y sea $g \in G$ de orden 2. Demuestre que una de las dos afirmaciones siguientes es verdadera:

(i) $\chi(g) \equiv \chi(1)$ (mód 4).
(ii) G tiene un subgrupo normal de índice 2.

EJERCICIO 12. Si G es cualquier grupo, demuestre que el conjunto de caracteres de grado 1 de G, con el producto natural $(\chi \cdot \chi')(\sigma) := \chi(\sigma)\chi'(\sigma)$, es un grupo.

EJERCICIO 13. En particular, si G es un grupo abeliano, el conjunto de caracteres irreducibles de G, denotado $\widehat{G}$, es un grupo abeliano. Demuestre que G y $\widehat{G}$ son isomorfos.

EJERCICIO 14. Escriba explícitamente la tabla de caracteres del grupo diédrico D_8.

EJERCICIO 15. Sea $G = \{1, i, j, k, -1, -i, -j, -k\}$, donde $i^2 = j^2 = k^2 = -1$, $ij = k, jk = i, ki = j, ji = -ij, kj = -jk, ik = -ki$. G es un grupo no abeliano de orden 8.

(1) Calcule la tabla de caracteres del grupo G. *Sugerencia:* El conjunto $N = \{1, -1\}$ es un subgrupo normal de G y el cociente $G/N = \{N, iN, jN, kN\}$ es isomorfo al grupo de Klein (que es abeliano).
(2) Observe que la tabla de caracteres de G y de D_8 son iguales.
(3) Sin embargo, muestre que los grupos G y D_8 no son isomorfos.

Así, la tabla de caracteres, en general, no puede discernir entre grupos no isomorfos.

EJERCICIO 16. Si $\rho : G \to \mathrm{GL}(V)$ es una representación de G y si χ es un carácter de G de grado 1, demuestre que la función θ en G, definida por

$$\theta(\sigma) := \chi(\sigma)\rho(\sigma)$$

es una representación de G. Más aún, si ψ es el carácter asociado a ρ, demuestre que el carácter asociado a θ es la función dada por $\chi(\sigma)\psi(\sigma)$.

EJERCICIO 17. Suponga que G es un grupo de orden impar.

(1) Demuestre que el único elemento de G que es conjugado de su inverso es el neutro $1 \in G$.
(2) Demuestre que si $\sigma \neq 1$ en G, entonces existe un carácter irreducible χ de G tal que $\chi(\sigma) \notin \mathbb{R}$.
(3) Demuestre que el carácter principal de G es el único carácter irreducible cuyos valores son reales.

EJERCICIO 18. Demuestre que un grupo finito de orden $8k$ debe tener al menos 5 clases de conjugación. *Sugerencia*: muestre que el grupo debe tener al menos 5 representaciones irreducibles.

Capítulo 15

Aplicaciones de la teoría de caracteres

DESPUÉS DE HABER DESARROLLADO los inicios de la teoría de caracteres de grupos finitos, la pregunta importante es: ¿qué información se puede obtener de un grupo finito a partir de sus caracteres? La respuesta es: *mucha*, y la ilustramos mostrando que la tabla de caracteres puede ser usada para determinar si un grupo es simple o soluble. Después de ésto, terminamos con algunas aplicaciones de la teoría de caracteres de grupos finitos probando algunos resultados importantes: uno de la teoría de caracteres (el grado de un carácter irreducible divide al orden del grupo), otro de la teoría de grupos finitos (el teorema $p^a q^b$ de Burnside) y al final el teorema de Frobenius que identifica un subgrupo normal de un grupo de permutaciones. Para probar los primeros dos resultados usaremos un poco de la teoría de números algebraicos que hemos recolectado en el apéndice, que aunque son temas que van más allá de lo desarrollado hasta ahora, creo que su lectura no es difícil y el lector se beneficiaría si lo intenta.

Para determinar la simpleza o solubilidad de un grupo necesitaremos los resultados siguientes:

LEMA 15.1. *Sean G un grupo finito y $H \lhd G$ un subgrupo normal.*

(1) *Si $\rho : G/H \to \mathrm{GL}(V)$ es una representación del cociente G/H, entonces la composición $\rho' : G \to G/H \to \mathrm{GL}(V)$ es una representación de G.*

(2) *El carácter χ' de ρ' es la composición del carácter χ de ρ con el homomorfismo canónico $\pi : G \to G/H$, i.e., $\chi' = \chi \circ \pi$.*

(3) *Si $W \subseteq V$ es un subespacio, entonces W es G-invariante si y sólo si es G/H-invariante.*

Demostración. La parte (1) es trivial. Para (2), si $g \in G$, como $\rho'(g) = \rho(gH)$, entonces

$$\chi'(g) = \mathrm{Tr}(\rho'(g)) = \mathrm{Tr}(\rho(gH)) = \chi(gH) = \chi(\pi(g)) = \chi \circ \pi(g).$$

Para (3), si $W \subseteq V$ es G-invariante, entonces para todo $gH \in G/H$ se tiene que

$$gH \cdot w = \{gh \cdot w \ : \ h \in H\} \subseteq W \quad \text{para todo } w \in W$$

ya que $gh \in G$. Se sigue que W es G/H-invariante.

Recíprocamente, si W es G/H-invariante, entonces para todo $g \in G$ y para todo $w \in W$, por definición de la acción $g \cdot w := (gH) \cdot w \in W$ y así W es G-invariante. □

Si G es un grupo finito y χ es un carácter de G, por 14.1(7) el conjunto

$$K_\chi := \{g \in G \,:\, \chi(g) = \chi(1)\}$$

es un subgrupo normal de G, al que se llama el *núcleo* de χ ya que es núcleo de la representación correspondiente por 14.1(7). Si χ_i son los caracteres irreducibles de G, escribiremos $K_i := K_{\chi_i}$.

PROPOSICIÓN 15.2. *Los subgrupos normales de G son los conjuntos de la forma $\bigcap_{i\in I} K_i$, para algún $I \subseteq \mathbb{I}_r = \{1, 2, \ldots, r\}$.*

Demostración. Supongamos que $H \lhd G$ y sean $\rho' : G/H \to \mathrm{GL}(V)$ la representación regular de G/H y χ' su carácter. Consideremos $\rho : G \to G/H \to \mathrm{GL}(V)$ y sea χ su carácter. Por el ejemplo 2 del capítulo 14,

$$\chi'(gH) = \begin{cases} 0 & \text{si } gH \neq H, \\ |G| & \text{si } gH = H \end{cases}$$

y así, como por el lema $\chi = \chi' \circ \pi$, entonces

$$\chi(g) = \chi'(gH) = \begin{cases} 0 & \text{si } g \notin H, \\ |G| & \text{si } g \in H \end{cases}$$

por lo que

$$(*) \qquad \chi(g) = \chi(1) \Leftrightarrow g \in H.$$

Se sigue que $K_\chi = H$. Ahora escribamos $\chi = \sum_i n_i \chi_i$, con $n_i \geq 0$ y χ_i los caracteres irreducibles de G. De 14.1(6) se tiene que

$$|\chi(g)| \leq \sum_i n_i |\chi_i(g)| \leq \sum_i n_i \chi_i(1) = \chi(1)$$

para todo $g \in G$. Se sigue que

$$(\dagger) \qquad g \in K_\chi \Leftrightarrow \chi(g) = \chi(1) \Leftrightarrow g \in K_i \text{ para todo } i \text{ tal que } n_i > 0$$

(ya que $|\chi_i(g)| \leq \chi_i(g)$ por 14.1(6)). Por lo tanto, de $(*)$ y $(\dagger)$ se sigue que

$$g \in H \Leftrightarrow g \in K_i \text{ para todo } i \text{ tal que } n_i > 0$$
$$\Leftrightarrow g \in \bigcap_{i\in I} K_i, \text{ donde } I = \{i \,:\, 1 \leq i \leq r \text{ y } n_i > 0\}.$$

Para el recíproco, como cada $K_i \lhd G$, para $i \in I$, entonces $\bigcap_{i\in I} K_i \lhd G$. □

Usando la proposición anterior, es bastante sencillo, mirando la tabla de caracteres de un grupo finito, decidir si es o no simple:

COROLARIO 15.3. *Un grupo finito G es simple si y sólo si el único carácter irreducible χ_i de G para el cual $\chi_i(g) = \chi_i(1)$, para algún $g \neq 1$ en G, es el carácter principal χ_1.*

Demostración. Si G es simple y si sucediera que $\chi_i(g) = \chi_i(1)$ para algún $i > 1$ y algún $g \neq 1$, entonces $g \in K_i \lhd G$, una contradicción.

Recíprocamente, si G no fuera simple, entonces existiría un $H \lhd G$ propio y con $H \neq 1$, i.e., existiría $g \neq 1$ en H. Por la proposición anterior, $H \subseteq K_i$ para algún $i > 1$ y por lo tanto $\chi_i(g) = \chi_i(1)$, en contradicción con la hipótesis. □

COROLARIO 15.4. *La tabla de caracteres de un grupo finito G se puede usar para determinar si G es o no soluble.*

Demostración. La tabla de caracteres de G nos da todos los núcleos K_i y la proposición anterior nos da todos los subgrupos normales de G y todas las relaciones de inclusión entre ellos, en términos de esos núcleos. Por lo tanto, la tabla de caracteres nos permite determinar todas las series normales de G y los órdenes de los términos involucrados. En particular, nos permite determinar si G tiene o no una serie normal cuyos cocientes sean abelianos. □

LEMA 15.5. *Si χ es un carácter irreducible de un grupo finito G, entonces para todo $g \in G$ el número complejo $[G : C_G(g)]\chi(g)/\chi(1)$ es un entero algebraico.*

Demostración. Sea $\rho : G \to \mathrm{GL}(W)$ una representación irreducible con carácter χ. Sean $g \in G$ y C_g su clase de conjugación. Consideremos la función

$$f : W \to W \qquad \text{dada por} \qquad f = \sum_{s \in C_g} \rho(s)$$

y observe que, para todo $\sigma \in G$ se tiene que $\rho(\sigma) \circ f = f \circ \rho(\sigma)$ ya que

$$\rho(\sigma)^{-1} f \rho(\sigma) = \sum_{s \in C_g} \rho(\sigma)^{-1}\rho(s)\rho(\sigma) = \sum_{s \in C_g} \rho(\sigma^{-1}s\sigma) = f,$$

la última igualdad por definición de f y porque $\sigma^{-1}s\sigma$ recorre C_g cuando s lo hace. Se sigue que $f\rho(\sigma) = \rho(\sigma)f$ como se quería. Podemos entonces aplicar el lema de Schur, 13.5(2), y así existe un escalar $\lambda \in \mathbb{C}$ tal que $f = \lambda \cdot \mathrm{id}_W$. Tomando trazas en esta igualdad obtenemos:

$$\begin{aligned} \lambda \cdot \chi(1) = \mathrm{Tr}(\lambda \cdot \mathrm{id}_W) = \mathrm{Tr}(f) = \mathrm{Tr}\Big(\sum_{s \in C_g} \rho(s)\Big) &= \sum_{s \in C_g} \chi(s) \\ &= \sum_{s \in C_g} \chi(g) \quad \text{ya que } \chi(s) = \chi(g) \text{ para todo } a \in C_g \\ &= |C_g|\chi(g) = [G : C_G(g)]\chi(g) \end{aligned}$$

y así $\lambda = [G : C_G(g)]\chi(g)/\chi(1)$.

Ahora, sea $R : G \to \mathrm{GL}(V)$ la representación regular de G y recordemos que como $\rho : G \to W$ es irreducible, la podemos ver, por 14.8, como una subrepresentación (irreducible) de R. Ahora, si $h : V \to V$ es la función lineal dada por $h = \sum_{s \in C_g} \rho(s)$, notamos que $h|_W = f$ y que $R(\sigma) \circ h = h \circ R(\sigma)$, para todo $\sigma \in G$ (lo cual se prueba en forma análoga a como lo hicimos para f) y como $f = \lambda \cdot \mathrm{id}_W$, entonces λ es un valor propio de h y así existe un $v \neq 0$ en $W \subseteq V$ tal que $h(v) = \lambda v$, por lo que si A es la matriz asociada a R, con respecto a la base $\{v_g\}_{g \in G}$ de V, se tiene que $\det(\lambda I_n - A) = 0$. Observamos ahora que, por el ejemplo 5 del capítulo 13, cada entrada de la matriz A de la representación regular es 0 ó 1. Se sigue que el polinomio característico $\phi(x) := \det(xI_n - A)$ es mónico con coeficientes enteros y como λ es raíz de este polinomio, entonces λ es un entero algebraico, como se quería. □

Una consecuencia importante es que el grado de cualquier representación irreducible divide al orden del grupo:

TEOREMA 15.6. *Si χ es un carácter irreducible de G, entonces $\chi(1)$ divide a $|G|$.*

Demostración. Sea $g_1, \ldots, g_r$ un conjunto completo de representantes de las clases de conjugación de G. Por el lema previo, $[G : C_G(g_i)]\chi(g_i)/\chi(1)$ es un entero algebraico para cada g_i, y por 14.1(5) y (4) también cada $\overline{\chi}(g_i)$ es un entero algebraico. Ahora, usando ortogonalidad por renglones, se tiene que

$$\frac{|G|}{\chi(1)} = \frac{1}{\chi(1)} \sum_{i=1}^{r} [G : C_G(g_i)]\chi(g_i)\overline{\chi}(g_i) = \sum_{i=1}^{r} [G : C_G(g_i)] \frac{\chi(g_i)}{\chi(1)} \overline{\chi}(g_i)$$

donde cada sumando en el lado derecho es un entero algebraico. Se sigue que el número racional $|G|/\chi(1)$ es un entero algebraico y por A.11 está en $\mathbb{Z}$, i.e., $\chi(1)$ divide a $|G|$. □

Para probar el teorema de Burnside, necesitaremos el lema siguiente:

LEMA 15.7. *Sean χ un carácter de G y $g \in G$. Pongamos $\gamma := \chi(g)/\chi(1)$. Si γ es un entero algebraico no nulo, entonces $|\gamma| = 1$.*

Demostración. Si n es el orden del elemento g, por 14.1(4), $\chi(g)$ es una suma de $\chi(1)$ raíces n-ésimas de la unidad, digamos $\chi(g) = \omega_1 + \cdots + \omega_{\chi(1)}$, y así

$$|\chi(g)| \leq |\omega_1| + \cdots + |\omega_{\chi(1)}| \leq \overbrace{1 + \cdots + 1}^{\chi(1)} = \chi(1)$$

y por lo tanto

$$|\gamma| = \frac{|\chi(g)|}{|\chi(1)|} \leq 1$$

y como $\gamma \neq 0$, entonces $0 < |\gamma|$. Si sucediera que $0 < |\gamma| < 1$, mostraremos que $\chi(g) = 0$. En efecto, sea $p(x) = x^t + a_{t-1}x^{t-1} + \cdots + a_1 t + a_0$ el polinomio mónico irreducible del cual γ es raíz. Por A.15, $p(x)$ tiene coeficientes en $\mathbb{Z}$. Ahora, como

$$\gamma = \frac{1}{d}(\omega_1 + \cdots + \omega_{\chi(1)}) \qquad \text{con } d := \chi(1) \text{ y } \omega_i \in \mu_n,$$

entonces, por A.10, todo conjugado algebraico γ' de γ es de la forma

$$\gamma' = \frac{1}{d}(\omega_1' + \cdots + \omega_{\chi(1)}'),$$

(donde los ω_j' son raíces de la unidad, porque son conjugados de ω_j que satisface $x^n - 1$), por lo que $0 < |\gamma| < 1$ implica que $0 < |\gamma'| \leq 1$ y así el producto de los conjugados algebraicos de γ (incluyendo a γ) satisface que

$$(*) \qquad \left| \prod \gamma' \right| < 1, \quad \text{ya que } |\gamma| < 1.$$

Pero, como los γ' son las raíces de $p(x)$, entonces el producto de éstas raíces es $\pm a_0$ (el término independiente de $p(x)$), i.e., $|a_0| < 1$ con $a_0 \in \mathbb{Z}$, por lo que $a_0 = 0$, y como $p(x)$ es irreducible, ésto implica que $p(x) = x$ y por lo tanto $\gamma = 0$ es su única raíz, i.e., $\chi(g)/\chi(1) = 0$ y así $\chi(g) = 0$, en contradicción con la hipótesis del lema. Se sigue que $|\gamma| = 1$. □

TEOREMA 15.8 (Burnside). *Sea G un grupo finito. Si G tiene una clase de conjugación cuyo orden es la potencia (no trivial) de un primo, entonces G no es simple.*

Demostración. Note que G no puede ser abeliano, ya que si lo fuera todas sus clases de conjugación tendrían un único elemento, en contradicción con la hipótesis del teorema.

Ahora, por hipótesis existe un elemento $1 \neq g$ en G cuya clase de conjugación es de orden p^t, para p un primo y $t \geq 1$ entero. De la ortogonalidad por columnas de la tabla de caracteres de G, se tiene que si $\chi_1, \ldots, \chi_r$ son los caracteres irreducibles de G, entonces

$$\begin{aligned} 0 &= \sum_{i=1}^{r} \chi_i(g)\overline{\chi_i}(1) && \text{ya que } g \neq 1 \text{ por lo que } \delta_{ij} = 0 \\ &= \sum_{i=1}^{r} \chi_i(g)\chi_i(1) && \text{porque } \chi_i(1) \text{ es real} \\ &= 1 + \sum_{i=2}^{r} \chi_i(g)\chi_i(1) && \text{ya que } \chi_1(g) = \chi_1(1) = 1 \text{ porque } \chi_1 \text{ es principal.} \end{aligned}$$

Dividiendo entre el primo p obtenemos

$$-\frac{1}{p} = \sum_{i=2}^{r} \chi_i(g)\chi_i(1)/p$$

y como $-1/p$ no es un entero algebraico, entonces uno de los sumandos $\chi_i(g)\chi_i(1)/p$ no es un entero algebraico, para $2 \leq i \leq r$, y como $\chi_i(g)$ sí es un entero algebraico, esto implica que $p \nmid \chi_i(1)$ (y también que $\chi_i(g) \neq 0$).

Ahora, como $[G : C_G(g)] = p^t$ y como $p \nmid \chi_i(1)$, entonces $[G : C_G(g)]$ es coprimo con $\chi_i(1)$ y así el 1 es combinación lineal de estos dos enteros:

$$1 = a[G : C_G(g)] + b\chi_i(1) \qquad \text{para algunos enteros } a, b.$$

Se sigue que

$$\frac{\chi_i(g)}{\chi_i(1)} = \frac{a[G : C_G(g)]\chi_i(g)}{\chi_i(1)} + b\chi_i(g)$$

donde, por el lema 15.5, el primer sumando de la derecha es un entero algebraico y como el segundo sumando también lo es, entonces $\chi_i(g)/\chi_i(1)$ es un entero algebraico $\neq 0$ y así, por el lema previo se sigue que su módulo es 1 por lo que $|\chi_i(g)| = |\chi_i(1)| = \chi_i(1)$. Ahora, sea $\rho_i : G \to \mathrm{GL}(W_i)$ la representación correspondiente al carácter χ_i. Observe que como, para $g \in G$, $\chi_i(g)$ es una suma de $\chi_i(1)$ raíces de la unidad, entonces

$$|\chi_i(g)| = \chi_i(1) \Leftrightarrow \rho_i(g) : W_i \to W_i \text{ tiene un único valor propio, digamos } \lambda_g,$$

ya que si $|\chi_i(g)| = \chi_i(1)$, como en la demostración del lema anterior, si n es el orden del elemento g, por 14.1(4), $\chi_i(g)$ es una suma de $\chi_i(1)$ raíces n-ésimas de la unidad, digamos ω_j, y así

$$|\chi_i(g)| = |\omega_1 + \cdots + \omega_{\chi_i(1)}| = \chi_i(1)$$

y, por la desigualdad del triángulo, la igualdad anterior sólo puede suceder si todos los w_i son iguales (a un ω, digamos, con módulo 1); se sigue que $\chi_i(g) = n_i\omega$, con $n_i = \chi_i(1)$, por lo que la matriz diagonal asociada a $\rho_i(g)$ tiene a ω en su diagonal n_i veces, y por lo tanto $\rho_i(g) = \omega\,\mathrm{id}_{W_i}$. Recíprocamente, si $\rho_i(g) = \lambda_g\,\mathrm{id}_{W_i}$, entonces λ_g es una raíz de la unidad y

$$|\chi_i(g)| = |\mathrm{Tr}(\lambda_g\,\mathrm{id}_{W_i})| = |n_i\lambda_g| = n_i = \chi_i(1)$$

como se quería. Así, $\rho_i(g)v = \lambda_g v$, para todo $v \in W_i$. Sea $K_i = \ker \rho_i \lhd G$. Como χ_i no es trivial, entonces $K_i \neq G$. Si $K_i \neq 1$, entonces G no sería simple y ya acabamos. Si $K_i = 1$, entonces ρ_i es inyectivo y observando ahora que la matriz de $\rho_i(g)$, con respecto a cualquier base de W_i, es una matriz diagonal con el único valor propio λ_g de $\rho_i(g)$ en la diagonal, se sigue que esta matriz conmuta con todas las matrices de la imagen $\rho_i(G)$ de ρ_i y así

$$\rho_i(gh) = \rho_i(g)\rho_i(h) = \rho_i(h)\rho_i(g) = \rho_i(hg)$$

para todo $h \in G$, y como ρ_i es inyectiva, la igualdad anterior implica que $gh = hg$ para todo $h \in G$, i.e., $g \in Z(G)$ por lo que $Z(G) \neq 1$. Pero $Z(G) \neq G$, porque G no es abeliano. Se sigue que $1 \neq Z(G) \lhd G$ y por lo tanto G no es simple. □

TEOREMA 15.9 (Burnside). *Si $|G| = p^r q^s$ con p, q primos, entonces G es soluble.*

Demostración. Por inducción sobre el orden de G (de hecho, sobre $r+s$). Si $r+s=1$, entonces $r=1$ y $s=0$, o viceversa; en cualquier caso G sería de orden primo y por lo tanto soluble. Supongamos ahora que $r+s>1$ y que el teorema es válido para grupos G de orden $p^a q^b$ con $a+b<r+s$. Sea Q un q-subgrupo de Sylow de G. Si $Q=1$, entonces G es un p-grupo y por lo tanto es soluble. Supongamos entonces que $Q \neq 1$; como Q es un q-grupo, su centro $Z(Q) \neq 1$ por 9.10, y así existe un $1 \neq g \in Z(Q)$, por lo que g conmuta con todos los elementos de Q y así $Q \subseteq C_G(g)$. Las inclusiones $Q \subseteq C_G(g) \subseteq G$ implican que $[G:Q] = [G:C_G(g)][C_G(g):Q]$ y como $|Q| = q^s$ (por ser un q-subgrupo de Sylow), entonces

$$[G:Q] = \frac{|G|}{|Q|} = \frac{p^r q^s}{q^s} = p^r.$$

Se sigue que $[G:C_G(g)]$ divide a p^r y así $[G:C_G(g)] = p^t$, para algún $t \leq r$.

CASO 1. Si $t=0$, $G = C_G(g)$ y así g conmuta con todos los elementos de G, por lo que $1 \neq g \in Z(G)$ y por lo tanto $1 \neq Z(G) \lhd G$, y como G no es abeliano $Z(G) \neq G$, y así G no es simple.

CASO 2. Si $t>0$, como $p^t = [G:C_G(g)]$ es el número de elementos en la clase de conjugación de g, por 8.2 y el ejemplo 12 del capítulo 8, entonces el teorema anterior implica que G no es simple.

En cualquiera de los dos casos hemos mostrado que G no es simple y así tiene un subgrupo normal propio $H \lhd G$ que, por el teorema de Lagrange, tienen orden de la forma $|H| = p^a q^b$ con $a+b<r+s$ y consecuentemente, por la hipótesis de inducción, H es soluble. El cociente G/H también tiene orden de la forma $p^\alpha q^\beta$ con $\alpha+\beta<r+s$, y por lo tanto también es soluble por la hipótesis de inducción. De 11.6(3) se sigue que G también es soluble. □

Caracteres inducidos y grupos de Frobenius. En 15.2 mostramos que la teoría de caracteres se puede usar para determinar los subgrupos normales de un grupo finito dado, sencillamente examinando las soluciones de la ecuación

$$\chi(\sigma) = \chi(1)$$

para un carácter arbitrario χ de G. Usando ésto, en esta última parte, probaremos un teorema de Frobenius que identifica un subgrupo normal de un grupo de permutaciones bajo ciertas condiciones y al final reformulamos este resultado en forma abstracta,

descomponiendo un grupo, bajo ciertas hipótesis en un producto. A diferencia del teorema p^aq^b de Burnside, para este teorema de Frobenius no existe una demostración sin usar teoría de caracteres y es una aplicación, hasta cierto punto más sencilla (no usa la teoría de números algebraicos), de la teoría de caracteres para probar un resultado de teoría de grupos *pura*. Antes de proceder al teorema de Frobenius, necesitaremos algunos resultados sobre caracteres.

Representaciones y caracteres inducidos. Si G es un grupo y $H \subseteq G$ es un subgrupo de índice finito, dada una representación de H, $\rho : H \to \mathrm{GL}(k, \mathbb{C})$, Frobenius [24] construye una representación de G que extiende a la representación de H dada, como sigue. Para extender ρ a G, primero se define $\rho(\sigma) = 0$ para $\sigma \in G - H$ y notamos que esta extensión de ρ a G *no* define una representación, tan sólo por el hecho de que si $\sigma \in G - H$, $\rho(\sigma) = 0$ no es invertible. Lo que Frobenius hace, usando el subgrupo H, es considerar la partición de G en clases laterales (digamos, izquierdas) de H,

$$G = g_1H \cup \cdots \cup g_nH$$

donde $n = [G : H]$ y los $g_1, \ldots, g_n$ son representantes dados de las clases laterales izquierdas de H en G. Luego, para cada $\sigma \in G$, define una matriz de tamaño $kn \times kn$ como un arreglo de $n \times n$ bloques de tamaño $k \times k$, donde cada bloque es la matriz $\rho(g_i^{-1}\sigma g_j)$, la cual es una matriz invertible si y sólo si $g_i^{-1}\sigma g_j \in H$, y es la matriz cero de tamaño $k \times k$ si $g_i^{-1}\sigma g_j \notin H$. Así, se ha definido una función $\rho^G : G \to \mathrm{GL}(kn, \mathbb{C})$ mediante

$$\rho^G(\sigma) := \begin{pmatrix} \rho(g_1^{-1}\sigma g_1) & \rho(g_1^{-1}\sigma g_2) & \cdots & \rho(g_1^{-1}\sigma g_n) \\ \rho(g_2^{-1}\sigma g_1) & \rho(g_2^{-1}\sigma g_2) & \cdots & \rho(g_2^{-1}\sigma g_n) \\ \vdots & & \ddots & \vdots \\ \rho(g_n^{-1}\sigma g_1) & \rho(g_n^{-1}\sigma g_2) & \cdots & \rho(g_n^{-1}\sigma g_n) \end{pmatrix}$$

LEMA 15.10. *La función $\rho^G : G \to \mathrm{GL}(kn, \mathbb{C})$ así definida es una representación de G.*

Demostración. Queremos probar que $\rho^G(\sigma\tau) = \rho^G(\sigma)\rho^G(\tau)$, para $\sigma, \tau \in G$. Comparando el bloque (i, j) en ambos lados de esta pretendida igualdad, el correspondiente al lado izquierdo es $\rho(g_i^{-1}\sigma\tau g_j)$ y el correspondiente al lado derecho, por definición de producto de matrices, es $\sum_{k=1}^{n} \rho(g_i^{-1}\sigma g_k)\rho(g_k^{-1}\tau g_j)$, y lo que queremos probar es

$$(*) \qquad \rho(g_i^{-1}\sigma\tau g_j) = \sum_{k=1}^{n} \rho(g_i^{-1}\sigma g_k)\rho(g_k^{-1}\tau g_j)$$

y se tienen dos casos, dependiendo del lado izquierdo:

CASO 1. Supongamos que $g_i^{-1}\sigma\tau g_j \notin H$. Entonces, el lado izquierdo de $(*)$ es la matriz cero. Para el lado derecho de $(*)$ veremos que, para cada k, ya sea que $g_i^{-1}\sigma g_k \notin$

H ó que $g_k^{-1}\tau g_j \notin H$. En efecto, suponiendo lo contrario se tiene que

$$g_i^{-1}\sigma\tau g_j = (g_i^{-1}\sigma g_k)(g_k^{-1}\tau g_j) \in H,$$

lo cual contradice lo que estamos asumiendo en este caso. Se sigue que cada sumando del lado derecho de $(*)$ es cero y por lo tanto se tiene la igualdad deseada.

CASO 2. Supongamos ahora que $v := g_i^{-1}\sigma\tau g_j \in H$. Considerando entonces al elemento τg_j, éste pertenece a única clase lateral, digamos g_tH, y así $\tau g_j = g_t u$ para algún $u \in H$. Entonces, $g_t^{-1}\tau g_j = u \in H$, y para $k \neq t$ se tiene que $\tau g_j \notin g_k H$ por lo que $g_k^{-1}\tau g_j \notin H$ y así el sumando correspondiente en el lado derecho de $(*)$ es cero; se sigue que el único sumando sobreviviente en el lado derecho de $(*)$ es cuando $k = t$, i.e.,

$$\rho(g_i^{-1}\sigma g_t)\rho(g_t^{-1}\tau g_j)$$

donde, para $v = g_i^{-1}\sigma\tau g_j \in H$ y $u = g_t^{-1}\tau g_j \in H$ se tiene que $vu^{-1} = g_i^{-1}\sigma g_t \in H$ por lo que la igualdad $(*)$ es equivalente a $\rho(v) = \rho(vu^{-1})\rho(u)$, la cual es verdadera porque u, v, vu^{-1} pertenecen a H y ρ es un homomorfismo. □

La representación $\rho^G : G \to \mathrm{GL}(kn, \mathbb{C})$, del lema anterior, se dice que es *inducida* de la representación $\rho : H \to \mathrm{GL}(k, \mathbb{C})$ del subgrupo H.

Ahora, si χ es el carácter de H asociado a ρ y si denotamos con χ^G al carácter de G correspondiente a ρ^G, se tiene que

$$(1) \qquad \chi^G(\sigma) = \mathrm{Tr}\rho^G(\sigma) = \sum_{i=1}^{n} \mathrm{Tr}\rho(g_i^{-1}\sigma g_i) = \sum_{i=1}^{n} \chi(g_i^{-1}\sigma g_i)$$

donde, si $g_i^{-1}\sigma g_i \notin H$ usamos la convención de que $\chi(g_i^{-1}\sigma g_i) = 0$ en conformidad con el hecho de que $\rho(g_i^{-1}\sigma g_i)$ es la matriz cero.

Observación. En la definición de ρ^G, y por lo tanto en la del carácter χ^G, usamos un sistema particular de representantes $g_1, \ldots, g_n$ de las clases laterales izquierdas de H en G. Veremos a continuación que el carácter χ^G no depende de la elección de estos representantes. Para ésto, supongamos que $\sigma_1, \ldots, \sigma_n$ son otros representantes, digamos $\sigma_i \in g_iH$, es decir, $\sigma_i = g_i h_i$ con $h_i \in H$. Se tiene entonces que

$$(\dagger) \qquad \sigma_i^{-1}\sigma\sigma_i = h_i^{-1}(g_i^{-1}\sigma g_i)h_i$$

con $h_i \in H$, por lo que $\sigma_i^{-1}\sigma\sigma_i \in H$ si y sólo si $g_i^{-1}\sigma g_i \in H$, y como estos elementos son conjugados en H por $(\dagger)$, entonces $\chi(\sigma_i^{-1}\sigma\sigma_i) = \chi(g_i^{-1}\sigma g_i)$, por lo que

$$\sum_{i=1}^{n} \chi(\sigma_i^{-1}\sigma\sigma_i) = \sum_{i=1}^{n} \chi(g_i^{-1}\sigma g_i) = \chi^G(\sigma)$$

como se quería.

Hay otras formas de escribir la fórmula para el carácter inducido χ^G. Por ejemplo, si $g_1H, \ldots, g_nH$ son las clases laterales izquierdas de H en G, podemos elegir como representantes a elementos de la forma $\sigma_i = g_iu$ con $u \in H$ fijo. Se tiene entonces que

$$\chi^G(\sigma) = \sum_{i=1}^{n} \chi((g_iu)^{-1}\sigma(g_iu)) = \sum_{i=1}^{n} \chi(u^{-1}g_i^{-1}\sigma g_iu) \tag{2}$$

y sumando sobre u en H, el lado izquierdo de (2) es constante y así queda multiplicado por $|H|$, mientras que el lado derecho de (2) al recorrer u el subgrupo H, como $G = g_1H \cup \cdots \cup g_nH$, los productos g_iu recorren todo el grupo G exactamente una vez y por lo tanto (2) queda $|H| \cdot \chi^G(\sigma) = \sum_{\tau \in G} \chi(\tau^{-1}\sigma\tau)$ y así

$$\chi^G(\sigma) = \frac{1}{|H|} \sum_{\tau \in G} \chi(\tau^{-1}\sigma\tau). \tag{3}$$

Ejemplo 1. Si $H \subseteq G$ es un subgrupo de índice finito n y si $g_1H, \ldots, g_nH$ son las clases laterales izquierdas de H en G, consideremos el carácter trivial ξ del subgrupo H, i.e., $\xi(h) = 1$ para todo $h \in H$; entonces, el carácter inducido ξ^G de G está dado por (1):

$$\xi^G(\sigma) = \sum_{i=1}^{n} \xi(g_i^{-1}\sigma g_i)$$

y para identificar este carácter de G, consideremos la representación por permutaciones de G dada por la acción de G en el conjunto G/H de clases laterales izquierdas de H en G mediante traslaciones izquierdas, i.e.,

$$G \times G/H \to G/H \qquad \text{dada por } (\sigma, g_iH) \mapsto (\sigma g_i)H$$

y sea χ el carácter de esta representación de G. Por el ejemplo 3 del capítulo 14 se tiene que $\chi(\sigma) = |(G/H)^\sigma|$ es el número de elementos g_iH de G/H fijados por σ. Observamos ahora que $\sigma g_iH = g_iH$ si y sólo si $g_i^{-1}\sigma g_i \in H$ por lo que el número $\chi(\sigma)$ de clases de G/H fijadas por σ es igual al número de elementos de la forma $g_i^{-1}\sigma g_i$ que están en H y este número es $\sum_{i=1}^{n} \xi(g_i^{-1}\sigma g_i)$ ya que cada uno de estos sumandos es 1 cuando $g_i^{-1}\sigma g_i \in H$ porque ξ es el carácter trivial. Hemos así identificado al carácter inducido ξ^G como el carácter χ, i.e., $\xi^G = \chi$.

Caracteres virtuales. Si G es un grupo finito y si $\chi_1, \ldots, \chi_r$ son todos los caracteres irreducibles de G, hemos visto en la observación (3) antes de 14.7 que todos los caracteres χ de G son combinaciones lineales de la forma

$$\chi = a_1\chi_1 + \cdots + a_r\chi_r \tag{*}$$

con los coeficientes a_i *enteros no negativos*, y en general, por 14.11 toda función de clases en G es una combinación lineal como la anterior pero con los coeficientes a_i en $\mathbb{C}$. Si ξ es una función de clases en G de la forma (*) pero con los coeficientes $a_i \in \mathbb{Z}$

enteros positivos, negativos o cero, diremos que ξ es un *carácter virtual* de G. Note que si hay coeficientes negativos, por la observación mencionada antes, la función ξ no es un carácter de G, i.e., no existe una representación de G cuya traza sea ξ. Ahora, si $\xi = a_1\chi_1 + \cdots + a_r\chi_r$ es un carácter virtual de G, entonces usando el producto interno definido antes de 14.4 se tiene que

$$\langle \xi, \xi \rangle = a_1^2 + \cdots + a_r^2$$

y por lo tanto, si $\langle \xi, \xi \rangle = 1$ entonces exactamente uno de los coeficientes en $\xi = a_1\chi_1 + \cdots + a_r\chi_r$ es ± 1 y los otros son cero. Hemos así probado:

PROPOSICIÓN 15.11. *Si ξ es un carácter virtual de G tal que $\langle \xi, \xi \rangle = 1$, entonces $\xi = \pm\chi$, donde χ es un carácter irreducible de G. Si además $\xi(1) > 0$, entonces $\xi = \chi$ es un carácter irreducible de G.*

□

Grupos de Frobenius. A continuación probaremos, usando teoría de caracteres, un celebrado teorema de Frobenius [27] que describe una clase importante de grupos, formulándolo en el lenguaje de acciones de grupos (grupos de permutaciones).

TEOREMA 15.12 (Frobenius). *Sea G un grupo finito que actúa transitivamente sobre un conjunto X de cardinalidad n. Si todas las permutaciones de G, excepto por la identidad, tienen a lo más un punto fijo, entonces el conjunto de elementos de G sin puntos fijos, junto con la identidad, es un subgrupo normal de G de orden n.*

NOTAS. La hipótesis nos dice que, para cada $\sigma \in G$, $|X^\sigma|$ es n, 1 ó cero. Podemos suponer que $X = \mathbb{I}_n$ y a los elementos σ de G los llamaremos *permutaciones* ya que su acción sobre los $k \in \mathbb{I}_n$ define la función $\sigma(k) = \sigma k$. Observe también que todo grupo finito G, en su representación regular, ocurre como un grupo de permutaciones en el cual ningún elemento del grupo, diferente de la identidad, tiene un punto fijo. Así, las hipótesis del teorema de Frobenius pueden verse como una pequeña variación de esta situación.

Demostración. Por la transitividad de la acción, existen permutaciones $p_i \in G$ tales que $p_1(1) = 1, p_2(1) = 2, \ldots, p_n(1) = n$. Podemos suponer que $p_1 = 1$ es la identidad de G. Ahora, el estabilizador de $i \in \mathbb{I}_n$ es el grupo

$$H_i = p_i H_1 p_i^{-1}$$

donde H_1 es el estabilizador del $1 \in \mathbb{I}_n$. En efecto, como $H_i = \{\sigma \in G : \sigma i = i\}$, si $\sigma \in H_1$, entonces

$$\begin{aligned} p_i \sigma p_i^{-1}(i) &= p_i \sigma(1) \quad \text{ya que } p_i(1) = i \\ &= p_i(1) \quad \text{ya que } \sigma \in H_1 \\ &= i \qquad \text{porque } p_i(1) = i, \end{aligned}$$

y así $p_i \sigma p_i^{-1} \in H_i$. Recíprocamente, si $\tau \in H_i$ note que

$$p_i^{-1} \tau p_i(1) = p_i \tau(i) = p_i(i) = 1$$

y así $p_i^{-1} \tau p_i \in H_1$, digamos $p_i^{-1} \tau p_i = u \in H_1$ y por lo tanto $\tau = p_i u p_i^{-1} \in p_i H_1 p_i^{-1}$, como se quería.

Por otra parte, si σH_1 es cualquier clase lateral izquierda de H_1 en G y si el representante σ manda 1 en i, entonces $\sigma \in p_i H_1$ y recíprocamente. En efecto, si σ manda 1 en i, sea $\tau \in H_1$ la permutación dada por $\tau(1) = 1$ y $\tau(j) = \sigma(j)$ si $j \neq 1$. Entonces, $\sigma = p_i \tau \in p_i H_1$, y el recíproco es claro.

Se sigue que $p_1 H_1, \ldots, p_n H_1$ son todas las clases laterales izquierdas de H_1 en G, y son diferentes entre sí porque si $p_i H_1 = p_j H_1$, entonces $p_i \in p_j H_1$ y así p_i manda 1 en i y también manda el 1 en j por lo que se debe tener que $i = j$. Entonces,

$$G = p_1 H_1 \cup p_2 H_1 \cup \cdots \cup p_n H_1$$

y $[G : H_1] = n$, por lo que el cardinal n de X (a veces se le llama el *grado* de G) divide a su orden, i.e., si $|G| = g$ y $|H_1| = h$, entonces $g = nh$.

Ahora, la hipótesis de que, excepto por la identidad, ninguna permutación de G tiene más de un punto fijo, en términos de estabilizadores, quiere decir que $H_i \cap H_j = 1$ para $i \neq j$.

Denotemos con $K^{\#} := K - \{1\}$ a los elementos $\neq 1$ de un grupo K. Entonces, para los estabilizadores H_i anteriores, $H_i^{\#}$ es el conjunto de permutaciones en G para las cuales i es el único punto fijo y así, si W es la colección de permutaciones sin puntos fijos, se tiene la partición de G:

$$G = \{1\} \cup W \cup H_1^{\#} \cup H_2^{\#} \cup \cdots \cup H_n^{\#}.$$

Observe ahora que $p_1 = 1$ es la única permutación con n puntos fijos y las permutaciones que fijan exactamente un punto están en la unión

$$H_1^{\#} \cup H_2^{\#} \cup \cdots \cup H_n^{\#}$$

y se tiene que $|H_i| = |H_1|$, por lo que $|H_i^{\#}| = h - 1$. Por lo tanto, G tiene $n(h-1)$ permutaciones que fijan un sólo punto y así el número de permutaciones sin puntos fijos es

$$|W| = |G| - |\{1\}| - |H_1^{\#} \cup H_2^{\#} \cup \cdots \cup H_n^{\#}| = g - 1 - n(h-1) = n - 1.$$

Con esta información sobre la estructura del grupo G, es fácil calcular el caracter inducido ψ^G de cualquier carácter ψ del subgrupo H_1. Recordemos que, por definición,

$$\psi^G(\sigma) := \sum_{i=1}^{n} \psi(p_i^{-1} \sigma p_i) \tag{1}$$

porque $G = p_1 H_1 \cup \cdots \cup p_n H_1$.

Ahora, si $d = \psi(1)$ es el grado de ψ, entonces usando (1), el grado de ψ^G es

$$\psi^G(1) = nd. \tag{2}$$

También, si $u_j \in H_j^{\#}$, como $H_j = p_j H_1 p_j^{-1}$, escribamos $u_j = p_j u p_j^{-1}$ con $u \in H_1$; note que $u \neq 1$ porque $u_j \neq 1$. Entonces,

$$\psi^G(u_j) = \sum_{i=1}^{n} \psi(p_i^{-1} p_j u p_j^{-1} p_i) \tag{3}$$

y el i-ésimo término de esta suma es $\neq 0$ si y sólo si $p_i^{-1} p_j u p_j^{-1} p_i \in H_1$, lo cual sucede si y sólo si $p_j u p_j^{-1} \in p_i H_1 p_i^{-1} = H_i$, i.e., si y sólo si $H_j = H_i$, i.e., si y sólo si $i = j$, por lo que (3) se reduce a

$$\psi^G(u_j) = \psi^G(p_j^{-1} u p_j) = \psi(u) \quad \text{para } j = 1, \ldots, n.$$

Finalmente, si $w \in W$, entonces

$$\psi^G(w) = 0 \tag{4}$$

porque $p_i^{-1} w p_i \notin H_1$ para todo i, ya que w no fija a punto alguno.

Resumiendo, los valores del carácter ψ^G, en 1, $u_j \in H_j^{\#}$ y $w \in W$, son:

$$\psi^G(1) = 1, \qquad \psi^G(u_j) = \psi(u), \qquad \psi^G(w) = 0.$$

Ahora, para el carácter χ de la representación por permutaciones de G, recordemos que $\chi(\sigma)$ es el número de puntos fijos de σ y así, para el carácter θ dado por $\theta(\sigma) = \chi(\sigma) - 1$, como para las permutaciones $1, u_j, w$ anteriores, los números de puntos fijos son n, 1 y cero, respectivamente, los valores de θ son los siguientes:

$$\theta(1) = n - 1, \qquad \theta(u_j) = 0, \qquad \theta(w) = -1.$$

Ahora, para el carácter virtual ξ dado por $\xi(\sigma) := \psi^G(\sigma) - d\theta(\sigma)$, usando los cálculos de ψ^G y θ anteriores, se tiene que

$$\xi(1) = dn - d(n-1) = d, \quad \xi(u_j) = \psi(u) - d0 = \psi(u), \quad \xi(w) = 0 - d(-1) = d$$

por lo que

$$\xi(w) = \xi(1) \qquad \text{para todo } w \in W. \tag{5}$$

Note que la igualdad (5) parece identificar W como el núcleo de ξ, sin embargo ésto no es así porque: (i) sólo caracteres verdaderos identifican núcleos (15.2) y ξ es un carácter virtual, (ii) pueden haber otros elementos fuera de W que satisfacen la ecuación (5).

El primer problema se resuelve si en lugar de tener cualquier carácter ψ de H_1 se toma un carácter *irreducible* ψ de H_1, digamos de grado d, en la definición (1), observando entonces que el carácter virtual ξ resulta en este caso un carácter irreducible

de grado d. En efecto, como estamos suponiendo que $\psi(1) = d$ y que $\langle \psi, \psi \rangle_{H_1} = 1$ porque ψ es irreducible, entonces

$$(6) \qquad \sum_{u \in H_1^{\#}} |\psi(u)|^2 = \sum_{u \in H_1} |\psi(u)|^2 - |\psi(1)|^2 = \sum_{u \in H_1} \langle \psi(u), \psi(u) \rangle - d^2 = h - d^2$$

la última igualdad porque $\langle \psi(u), \psi(u) \rangle = 1$ y $|H_1| = h$. Ahora, como $\xi(1) = d > 0$, para probar que ξ es un carácter irreducible de G, de grado d, por 15.11 basta ver que $\langle \xi, \xi \rangle = 1$. Ahora, como $G = \{1\} \cup W \cup (H_1^{\#} \cup \cdots \cup H_n^{\#})$, entonces

$$\begin{aligned} \sum_{\sigma \in G} |\xi(\sigma)|^2 &= |\xi(1)|^2 + \sum_{w \in W} |\xi(w)|^2 + \sum_{j=1}^{n} \Big(\sum_{u_j \in H_j^{\#}} |\xi(u_j)|^2 \Big) \\ &= d^2 + (n-1)d^2 + n(h - d^2) = nh = g. \end{aligned}$$

(porque $|W| = n - 1$ y $\xi(w) = d$ para $w \in W$, y por (6)). Se sigue que

$$\langle \xi, \xi \rangle = \frac{1}{|G|} \sum_{\sigma \in G} |\xi(\sigma)|^2 = \frac{1}{g}(g) = 1$$

y así, por 15.11, ξ es un carácter irreducible de G.

Para resolver el segundo problema, cambiaremos el carácter ξ en (5) por otro carácter π para el cual $W \cup 1 = \ker \pi$. Para hacer ésto, sean $\psi_1, \ldots, \psi_r$ todos los caracteres irreducibles de H_1 y sean $d_i = \psi_i(1)$ sus grados. Para el carácter ρ de la representación regular de H_1 sabemos que $\rho(1) = h$, $\rho(u) = 0$ para $u \neq 1$ y

$$(7) \qquad \rho = \sum_{k=1}^{r} d_k \psi_k.$$

Definiendo ahora caracteres ξ_k de G en forma análoga a como se definió ξ sólo que ahora usando ψ_k en lugar de ψ, i.e., $\xi_k = \psi_k^G - d_k \theta$, para $k = 1, \ldots, r$, notamos que los valores de ξ_k son análogos a los de ξ, i.e.,

$$(8) \qquad \xi_k(1) = d_k, \qquad \xi_k(u_j) = \psi_k(u), \qquad \xi_k(w) = d_k.$$

Se define entonces el carácter π mediante $\pi := \sum_{k=1}^{r} d_k \xi_k$ (es un carácter porque los $d_k \geq 1$ son enteros) y substituyendo los valores de ξ_k se tiene que

$$\pi(1) = \sum_{k=1}^{r} d_k \xi_k(1) = \sum_{k=1}^{r} d_k^2 = h \quad \text{(por (8))}$$

$$\pi(u_j) = \sum_{k=1}^{r} d_k \xi_k(u_j) = \sum_{k=1}^{r} d_k \psi_k(u) = \rho(u) = 0 \quad \text{(por (8), (7) y la línea arriba de (7))}$$

$$\pi(w) = \sum_{k=1}^{r} d_k \xi_k(w) = \sum_{k=1}^{r} d_k^2 = h \quad \text{(por (8))}$$

y por lo tanto $\pi(w) = \pi(1)$ si y sólo si $w \in W$, por lo que para este carácter π se tiene que su núcleo es en efecto $\{1\} \cup W$ y así, por (15.2), $\{1\} \cup W$ es un subgrupo normal de G de orden n, como se quería. □

Ejemplo 2. Para el grupo $G = S_3$ que actúa transitivamente en $\mathbb{I}_3$, escribiendo (ejemplo 3, capítulo 4), $S_3 = \{1, (12), (13), (23), (123), (132)\}$, se tiene que

$$\mathbb{I}_3^1 = \mathbb{I}_3,\ \mathbb{I}_3^{(12)} = \{3\},\ \mathbb{I}_3^{(13)} = \{2\},\ \mathbb{I}_3^{(23)} = \{1\},\ \mathbb{I}_3^{(123)} = \emptyset = \mathbb{I}_3^{(132)}$$

y el teorema de Frobenius nos dice que el conjunto $\{(123), (132)\}$ junto con la identidad es un subgrupo normal de S_3. Es decir,

$$\{1, (123), (132)\} \lhd S_3$$

y notamos que este subgrupo es A_3.

El teorema anterior se puede reformular, en forma abstracta, como sigue:

TEOREMA 15.13 (Frobenius). *Si H es un subgrupo de un grupo finito G con la propiedad de que $\sigma H \sigma^{-1} \cap H = 1$, para todo $\sigma \in G - H$, entonces G tiene un subgrupo normal K tal que $G = KH$ y $H \cap K = 1$. (Es decir, G es el producto semidirecto de K y H).*

Demostración. Para aplicar el teorema anterior lo primero que haremos será ver al grupo abstracto G como un grupo de permutaciones. Para ésto, consideremos la acción de G en el conjunto de clases laterales izquierdas G/H, dada por $(\sigma, gH) \mapsto \sigma gH$ y la representación por permutaciones correspondiente $\rho : G \to \mathrm{GL}(n, \mathbb{C})$, donde $n = [G : H]$ y hemos elegido una partición de G en clases laterales de H, $G = g_1 H \cup \cdots \cup g_n H$, con $g_1 = 1$. Recuerde que $\rho(\sigma)$ manda la clase $g_i H$ en $\sigma g_i H$, por lo que la clase $g_i H$ permanece fija bajo la acción de $\rho(\sigma)$, i.e., $\sigma g_i H = g_i H$, si y sólo si $g_i^{-1} \sigma g_i H = H$, i.e., si y sólo si $\sigma \in g_i H g_i^{-1}$. Veremos que la representación ρ es fiel, i.e., es inyectiva. En efecto, si $\sigma \neq 1$ observe que $\rho(\sigma)$ no puede tener más de un punto fijo, ya que si $g_i H$ y $g_j H$ quedan fijas bajo $\rho(\sigma)$, entonces $1 \neq \sigma \in g_i H g_i^{-1} \cap g_j H g_j^{-1}$, y por lo tanto

$H \cap g_i^{-1} g_j H g_j^{-1} g_i \neq 1$, en contradicción con la hipótesis del teorema porque al estar suponiendo que $g_i H \neq g_j H$ se tiene que $g_i^{-1} g_j \notin H$. Esto nos dice que ρ es inyectiva y por lo tanto G es isomorfo a su imagen, que es el subgrupo de permutaciones de la forma

$$\begin{pmatrix} g_1 H & \cdots & g_n H \\ \sigma g_1 H & \cdots & \sigma g_n H \end{pmatrix}$$

y es claro que este grupo actúa transitivamente. También, al probar la inyectividad de ρ mostramos que ningún elemento de G, con la excepción del 1, fija a más de un elemento, y así, por el teorema anterior el conjunto $K = 1 \cup W$, con W la familia de elementos de G sin puntos fijos, es un subgrupo normal de G de orden $n = [G : H]$.

Veremos ahora que los elementos de K están en correspondencia biyectiva con las clases laterales en G/H. En efecto, como cada elemento de G pertenece a una única clase lateral, se tiene la función $K \to G/H$, la cual afirmamos que es inyectiva. Para ver ésto, supongamos que $w, w' \in K$ son tales que pertenecen a la misma clase $g_i H$; entonces, $w, w' \in K \cap g_i H$ y así $w^{-1} w' \in H$ y por lo tanto fija a la clase lateral $1H = H$. Pero como $w^{-1} w' \in K$, porque K es grupo, y como el único elemento de K que fija algo es el 1, entonces $w^{-1} w' = 1$, i.e., $w = w'$, por lo que la función $K \to G/H$ es inyectiva. Finalmente, como $|K| = n = |G/H|$, entonces la función inyectiva anterior debe ser suprayectiva. Podemos entonces denotar los elementos de K como $w_1 = 1, w_2, \ldots, w_n$, donde los $w_i \in g_i H$, de tal forma que los w_i se pueden usar como representantes de las clases laterales de H en G en lugar de los g_i. Se sigue que $G = KH$. Por otra parte, se tiene que $H \cap K = 1$ porque los elementos de K están en correspondencia biyectiva con G/H y así los elementos de H corresponden al 1 de K. □

Cuando un grupo finito G tiene un subgrupo H que satisface el teorema anterior, se dice que G es un *grupo de Frobenius* y que H es un *complemento de Frobenius*; al subgrupo normal K cuya existencia asegura el teorema anterior, se le llama un *núcleo de Frobenius*.

Ejemplo 3. Si $G = D_{2n}$ es un grupo diédrico con n *impar* y $H \subseteq D_{2n}$ es cualquier subgrupo de orden 2, entonces D_{2n} es un grupo de Frobenius con complemento H.

Observación. En la demostración del teorema 15.13 se usó el teorema 15.12. Mostraremos ahora que, de hecho, el teorema 15.13 implica el teorema 15.12. En efecto, supongamos que G actúa transitivamente en X y para $x \in X$ sea $H = G_x$ el estabilizador correspondiente. Como la acción de G en X es transitiva, por el teorema órbita-estabilizador 8.2, se tiene que $[G : H] = n = |X|$ y la acción de G se puede ver como la acción de G en G/H mediante traslaciones izquierdas. Por otra parte, como el estabilizador de una clase lateral σH es $\sigma H \sigma^{-1}$, la hipótesis de que ningún elemento de G fija dos o más elementos, i.e., que la intersección de dos estabilizadores es trivial,

implica que, para todo $g \in G$, $gHg^{-1} \cap H = 1$ ó $gHg^{-1} \cap H = H$, donde el primer caso sucede cuando $g \in G - H$. Por el teorema 15.13 se sigue que G tiene un subgrupo normal K tal que $G = KH$ y $H \cap K = 1$ y por la demostración del mismo teorema se tiene que K se puede identificar con G/H. Note entonces que $\sigma gH = gH$ si y sólo si $\sigma g = gh$, con $h \in H$, i.e., si y sólo si $\sigma = ghg^{-1} \in gHg^{-1}$; por lo tanto, σ fija a la clase lateral gH si y sólo si $\sigma \in gHg^{-1}$. Si sucediera que σ fija dos clases laterales g_1H y g_2H en G/H, entonces $\sigma \in g_1Hg_1^{-1} \cap g_2Hg_2^{-1} = 1$ (la intersección es trivial porque G es Frobenius con complemento H). Se sigue que el número de puntos fijos en G/H de $\sigma \in G$ es:

$$|(G/H)^\sigma| = \begin{cases} n = [G:H] & \text{si } \sigma = 1, \\ 0 & \text{si } \sigma \neq 1 \text{ y } \sigma \in K, \\ 1 & \text{si } \sigma \in \bigcup_{g \in G} gHg^{-1}, \end{cases}$$

por lo que $K = 1 \cup W$, con W el subconjunto de G sin puntos fijos, como se quería.

Notas. (1) Existen grupos simples de orden $p^aq^br^c$, con p, q, r primos, el menor de ellos es el grupo alternante A_5 de orden $60 = 2^2 \cdot 3 \cdot 5$.

(2) En su libro, Burnside [2] había demostrado algunos casos especiales de su teorema y después de estudiar la teoría de caracteres de Frobenius, en [25] obtuvo la demostración que presentamos en este capítulo, como una de las más célebres aplicaciones de la teoría de caracteres. Como mencionamos antes, fue hasta 1972 cuando H. Bender [23] encontró una demostración, sin usar caracteres, del teorema de Burnside.

(3) Todas las demostraciones, conocidas hasta ahora, del teorema de Frobenius [38], usan teoría de caracteres en una forma u otra. El teorema de Frobenius junto con el teorema p^aq^b de Burnside son modelos de cómo usar teoría de caracteres para obtener información sobre la estructura de grupos finitos.

(4) El teorema de Frobenius 15.13 tiene una demostración, que no usa caracteres, en los dos casos siguientes:

(1) El orden del subgrupo H es *par*.
(2) El subgrupo H es *soluble*.

Note que, por el teorema de Feit y Thompson (vea la nota 2 al final del capítulo 11), todo grupo finito de orden impar es soluble, por lo que los dos casos anteriores son todas las posibilidades para H y así la demostración de estos dos casos es una demostración del teorema de Frobenius, sin embargo el teorema de Feit-Thompson no sólo usa caracteres en su demostración, sino que es de una profundidad mayor. El caso (2), cuando el complemento de Frobenius H es soluble, ya había sido demostrado por Burnside en

[26]. La demostración que damos se basa en Grün [41] y Shaw [53]. A continuación daremos demostraciones de los casos (1) y (2) de arriba.

CASO 1. [H. Bender]. Supongamos que $|H|$ es par y que $H \cap gHg^{-1} = 1$ para todo $g \in G - H$ (y por lo tanto $H = N_G(H)$ porque si $g \in N_G(H)$ entonces $gHg^{-1} = H$, y si g no estuviera en H, entonces $H \cap gHg^{-1} = 1$ por lo que $H \cap H = 1$, en contradicción con la hipótesis de que $H \neq 1$; se sigue que $N_G(H) \subseteq H$ y la otra inclusión siempre se da). Ahora, si $[G : H] = n$, como $N_G(H) = H$, entonces H tiene exactamente n conjugados en G, digamos $H_1, \ldots, H_n$, cada uno de éstos tiene orden $|H|$ que es par y por lo tanto podemos escoger elementos $\sigma_j \in H_j$ tales que $\sigma_j \neq 1$ y $\sigma_j^2 = 1$. Mostraremos que para cada j,

$$(*) \qquad \{\sigma_j\sigma_i \ : \ i = 1, \ldots, n\} = G - \bigcup_{k=1}^{n} H_k.$$

En efecto, para la inclusión del lado izquierdo en el lado derecho, supongamos que esto no es así, i.e., que existe un $\sigma_j\sigma_i \in H_k$ para algún $j \neq i$ y algún k. Se tiene entonces que $H_j \cap H_i = 1$ ya que $H_j \cap H_i = g_j H g_j^{-1} \cap g_i H g_i^{-1}$ y si esta intersección fuera $\neq 1$, entonces conjugando con g_j^{-1} se tendría que $H \cap (g_j^{-1}g_i)H(g_j^{-1}g_i)^{-1} \neq 1$, donde $g_j^{-1}g_i \notin H$ ya que de lo contrario $g_j^{-1}g_i = h \in H$ y por lo tanto $g_i = g_j h$ y así $g_i H g_i^{-1} = g_j h H h^{-1} g_j^{-1} = g_j H g_j^{-1}$, i.e., $H_i = H_j$, una contradicción. Ahora, $H_j \cap H_i = 1$ implica que $\sigma_j\sigma_i \neq 1$ ya que si $\sigma_j\sigma_i = 1$ entonces $\sigma_i = \sigma_j^{-1} \in H_j$ por lo que $\sigma_i \in H_i \cap H_j = 1$, en contradicción con $\sigma_i \neq 1$. Se tiene entonces que

$$1 \neq \sigma_j(\sigma_j\sigma_i)\sigma_j^{-1} = \sigma_j^2\sigma_i\sigma_j = \sigma_i\sigma_j = \sigma_i^{-1}\sigma_j^{-1} = (\sigma_j\sigma_i)^{-1}$$

porque $\sigma_j^2 = 1$ y así $\sigma_j^{-1} = \sigma_j$ y lo mismo para σ_i. Se sigue que $\sigma_j(\sigma_j\sigma_i)\sigma_j^{-1} = (\sigma_j\sigma_i)^{-1}$ está en $\sigma_j H_k \sigma_j^{-1}$ y como $\sigma_j\sigma_i \in H_k$, entonces $(\sigma_j\sigma_i)^{-1} \in H_k$, por lo que

$$1 \neq \sigma_j(\sigma_j\sigma_i)\sigma_j^{-1} \in H_k \cap \sigma_j H_k \sigma_j^{-1},$$

lo cual por hipótesis sólo puede suceder si $\sigma_j \in H_k$, i.e., si $j = k$. En forma análoga se prueba que $i = k$, pero esto contradice el hecho de que $i \neq j$. Se sigue que $\sigma_j\sigma_i \notin H_k$ para todo $k = 1, \ldots, n$, y así

$$(**) \qquad \{\sigma_j\sigma_i \ : \ i = 1, \ldots, n\} \subseteq G - \bigcup_{k=1}^{n} H_k.$$

Ahora, como $|H_k| = |H|$ y hay $[G : H]$ de los H_k, que sólo coinciden en el 1, entonces

$$|G - \bigcup_{k=1}^{n} H_k| = |G| - [G : H](|H| - 1) = |G| - [G : H]|H| + [G : H] = [G : H] = n$$

y como $|\{\sigma_j\sigma_i \ : \ i = 1, \ldots, n\}| = n$ porque σ_j está fijo, entonces la inclusión (**) debe ser una igualdad, como se quería, y esto para cada $j = 1, \ldots, n$.

Mostraremos ahora que $N = \{\sigma_j\sigma_i \ : \ i = 1, \ldots, n\}$ es un subgrupo normal de G. En efecto, $1 \in N$ porque $\sigma_j\sigma_j = \sigma_j^2 = 1$. Ahora, si $a, b \in N$, escribamos $a = \sigma_1\sigma_i$ para algún i y escogiendo $j = 1$ en $(*)$, y $b = \sigma_i\sigma_k$ para algún k y escogiendo $j = i$ en $(*)$. Entonces, $ab = \sigma_1\sigma_i\sigma_i\sigma_k = \sigma_1\sigma_k \in N$, i.e., N es cerrado bajo productos. Ahora, si $a = \sigma_j\sigma_i \in N$, entonces $a^{-1} = \sigma_i\sigma_j \in N$ y así N es un subgrupo de G. Para ver que N es normal en G, sean $a \in N$ y $\sigma \in G$. Si $\sigma \in N$, claramente $\sigma a\sigma^{-1} \in N$. Si $\sigma \notin N$, entonces $\sigma \in H_k$ para algún k y supongamos que $\sigma a\sigma^{-1} \notin N$, es decir que $\sigma a\sigma^{-1} = \sigma_t \in H_t$ para algún t. Entonces, $a = \sigma^{-1}\sigma_t\sigma \in N$, y como $\sigma_t \in H_t = gHg^{-1}$, entonces $\sigma_t = ghg^{-1}$ por lo que $a = \sigma^{-1}\sigma_t\sigma = \sigma^{-1}ghg^{-1}\sigma = (\sigma^{-1}g)h(\sigma^{-1}g)^{-1}$ pertenece a un conjugado de H, en contradicción con $a \in N$. Se sigue que $\sigma a\sigma^{-1} \in N$, por lo que $N \lhd G$.

Es claro que $N \cap H = 1$, ya que si $1 \neq x \in N \cap H$, entonces $x \in H$ y así está en un conjugado de H y en N, una contradicción. Finalmente, como $|N| = [G : H]$, entonces $|G| = |N||H|$ y como $N \cap H = 1$, esto implica que $G = NH$. □

CASO 2. [O. Grün, R. H. Shaw]. Supongamos que H es *soluble* y que $H \cap gHg^{-1} = 1$ para todo $g \in G - H$. Escojamos representantes de las clases laterales izquierdas de H en G, de tal manera que

$$G = x_1H \cup \ldots \cup x_nH, \qquad n = [G : H]$$

y consideremos la acción de G mediante traslaciones izquierdas en G/H. Los ciclos de la acción de $g \in G$ son $(x_jH, gx_jH, \ldots, g^{r_j-1}x_jH)$, para $j = 1, \ldots, n$ y donde $g^{r_j}x_jH = x_jH$. Escribamos $H' := [H, H]$ y consideremos el *homomorfismo de transferencia*[1] $V : G \to H/H'$, dado por

$$V(g) := \prod_{j=1}^{n} x_j^{-1}g^{r_j}x_jH'$$

donde $x_1H, \ldots, x_nH$, $n = [G : H]$, son las clases laterales izquierdas de H en G; podemos suponer que $x_1 = 1$. Entonces,

(1). Si $h \in H$, entonces $V(h) = hH'$ (por lo tanto, $H \cap \ker V = H'$). En efecto, $V(h) = \prod_{j=1}^{n} x_j^{-1}h^{r_j}x_jH'$, donde $x_1 = 1$ y $x_j^{-1}h^{r_j}x_j \in H$. Como $x_1 = 1$ y $h \in H$, entonces $H = x_1H = hx_1H$, por lo que $r_1 = 1$. Ahora, si $j > 1$, entonces $x_j^{-1}h^{r_j}x_j \in H \cap x_j^{-1}Hx_j = 1$. Se sigue que $V(h) = hH'$, como se quería.

(2). $G = \ker V \cdot H$. En efecto, si $g \in G$, escribamos $V(g) = hH' \in H/H'$. Por la parte (1), para esta $h \in H$ se tiene que $hH' = V(h)$ y así $V(g) = V(h)$ y por lo tanto $gh^{-1} \in \ker V$, digamos $gh^{-1} = u \in \ker V$ y así $g = uh$, con $u \in \ker V$ y $h \in H$, es decir, $G = \ker V \cdot H$.

[1] Para la definición del homomorfismo de transferencia, vea la sección inmediata al final de esta demostración.

(3). Pongamos $K = \ker V \lhd G$. Por la parte (1) se tiene que $K \cap H = H'$ y como H es soluble $H' \subsetneq H$.

(i). Si $H' = 1$, ya acabamos.

(ii). Si $H' \neq 1$, probaremos, por inducción sobre el orden de G que

$$N := G - \bigcup_{g \in G} gHg^{-1}$$

es un subgrupo normal de G y que $G = NH$ con $N \cap H = 1$.

Para ésto, observando que $H' \subseteq K$, mostraremos que K es un grupo de Frobenius con complemento H'. En efecto, si $g \in K - H'$, de la igualdad $K \cap H = H'$ se sigue que $g \in G - H$ y por lo tanto $H' \cap gH'g^{-1} \subseteq H \cap gHg^{-1} = 1$, es decir, K y H' satisfacen las condiciones del caso 2 (ya que K también es soluble) y como $K \subsetneq G$ (ya que de lo contrario se tendría que $H = 1$ y por lo tanto $H' = 1$), entonces por hipótesis de inducción el conjunto

$$F := K - \bigcup_{g \in K} gH'g^{-1}$$

es un subgrupo normal de K tal que $K = FH'$ y $F \cap H' = 1$. Se tiene entonces que:

$$\begin{aligned}
|F| &= [K : H'] && \text{porque } K = FH' \text{ y } F \cap H' = 1 \\
&= [K : K \cap H] && \text{ya que } H' = K \cap H \\
&= [KH : H] && \text{por el segundo teorema de isomorfismo de Noether} \\
&= [G : H] && \text{ya que } G = KH \text{ por (2)} \\
&= |N| && \text{por la demostración del caso 1.}
\end{aligned}$$

Ahora, si $g = kh \in KH = G$, entonces

$$\begin{aligned}
F \cap gHg^{-1} &= F \cap (kh)Hh^{-1}k^{-1} = F \cap kHk^{-1} \\
&= F \cap (K \cap kHk^{-1}) && \text{porque } F \subseteq K \text{ y así } F \cap K = F \\
&= F \cap (kKk^{-1} \cap kHk^{-1}) \\
&= F \cap k(K \cap H)k^{-1} \\
&= F \cap kH'k^{-1} && \text{por (1) ó (3)} \\
&= kFk^{-1} \cap kH'k^{-1} && \text{porque } F \lhd K \\
&= k(F \cap H')k^{-1} \\
&= 1 && \text{porque } F \cap H' = 1.
\end{aligned}$$

Por lo tanto,

$$F \subseteq G - \bigcup_{g \in G} gHg^{-1} = N$$

y como $|F| = |N|$, entonces $F = N$ y es claro que $N \lhd G$, $G = NH$ y $N \cap H = 1$. □

El homomorfismo de transferencia. Si H es un subgrupo de índice finito n de un grupo G y si $g_1, \ldots, g_n$ es un conjunto completo de representantes de las clases laterales izquierdas de H en G, dado un elemento $g \in G$ y un representante g_i, el producto gg_i pertenece a una única clase lateral, digamos $g_{j(g)}H$ y note que este hecho implica que la función $j(g)$ recorre todo el conjunto de índices $\mathbb{I}_n$ cuando i lo hace. Escribamos entonces $gg_i = g_{j(g)}h_i(g)$, para $h_i(g) \in H$, donde la notación indica que este elemento depende de i, es decir, de g_i, y de g. Los elementos $h_i(g) = g_{j(g)}^{-1}gg_i$ dependen de g y de los representantes g_i, pero más adelante veremos que su producto, para $1 \leq i \leq n$, no depende del conjunto de representantes de las clases laterales izquierdas de H. Por el momento, usando este particular conjunto de representantes $g_1, \ldots, g_n$, definamos la función $V : G \to H/H'$, donde $H' = [H : H]$ es el subgrupo conmutador de H, mediante

$$V(g) := \prod_{i=1}^{n} h_i(g) \pmod{H'}$$

donde recordamos que el cociente H/H' es un grupo abeliano y mód H' quiere decir que estamos tomando clases laterales de H' en H.

TEOREMA 15.14. *Sean G un grupo, H un subgrupo de índice finito n, $g_1, \ldots, g_n$ un conjunto completo de representantes de las clases laterales izquierdas de H en G y sea $V : G \to H/H'$ la función anterior. Entonces,*

(1) *V es un homomorfismo, al que se llama el* homomorfismo de transferencia.

(2) *La definición de V es independiente del conjunto completo de representantes de las clases laterales izquierdas de H en G.*

Demostración. (1): Si $g, t \in G$ y si $gg_i = g_{j(g)}h_i(g)$ y $tg_i = g_{j(t)}h_i(t)$, entonces

$$V(g)V(t) = \left(\prod_{i=1}^{n} h_i(g)\right)\left(\prod_{i=1}^{n} h_i(t)\right)H' \tag{1.1}$$

y si $(gt)g_i = g_{j(gt)}h_i(gt)$, entonces

$$V(gt) = \left(\prod_{i=1}^{n} h_i(gt)\right)H' \tag{1.2}$$

y denotando por u el producto de los términos entre paréntesis del lado derecho de (1.1) y por v el término entre paréntesis del lado derecho de (1.2), para probar que V es un homomorfismo lo que debemos probar es que $u \equiv v \pmod{H'}$, es decir, debemos probar que $uv^{-1} \in H'$, i.e., que $u = kv$ para algún $k \in H'$. Para probar ésto, supongamos por un momento que v es igual al producto de los $2n$ elementos $h_i(g)$, $h_i(t)$, $1 \leq i \leq n$, en *algún orden*. Observe entonces que al considerar este producto

en el cociente H/H', como éste es abeliano, cualquier rearreglo de los términos del producto anterior no afecta su clase lateral en H/H', y como u es un producto de estos $2n$ términos entonces se tendrá que $v \equiv u \pmod{H'}$ como se quería. Basta mostrar entonces que v es el producto de los $2n$ términos $h_i(g)$, $h_i(t)$ en algún orden y para ésto observe primero que, por definición de $h_i(gt)$, se tiene que

$$(gt)g_i = g_{j(gt)}h_i(gt) \tag{1.3}$$

y por otro lado

$$(gt)g_i = g(tg_i) = gg_{j(t)}h_i(t) = g_{j(g)}h_{j(t)}h_i(t) \tag{1.4}$$

y de (1.3) y (1.4) obtenemos

$$g_{j(gt)}h_i(gt) = g_{j(g)}h_j(g)h_i(t)$$

y como los $g_1, \ldots, g_n$ son un conjunto completo de representantes de las clases laterales izquierdas de H en G, se debe tener que $g_{j(gt)} = g_{j(g)}$ y por lo tanto

$$h_i(gt) = h_{j(t)}(g)h_i(t), \quad 1 \leq i \leq n. \tag{1.5}$$

Ahora, como $v = \prod h_i(gt)$, el resultado deseado se seguirá de (1.5) una vez que mostremos que $j(t)$ recorre el conjunto $\mathbb{I}_n$, en algún orden, cuando i lo hace, pero esto fue lo que observamos al principio de ésta sección. Esto termina la demostración de la parte (1).

(2): Supongamos ahora que $\sigma_1, \ldots, \sigma_n$ es otro conjunto completo de representantes de las clases laterales izquierdas de H en G, las cuales podemos suponer que las numeramos de tal forma que $g_iH = \sigma_iH$. Dado $g \in G$, como $V(g) = \prod h_i(g)H'$, para $gg_i = g_{j(g)}h_i(g)$, si escribimos $g\sigma_i = \sigma_{j(g)}\tilde{h}_i(g)$, notando que el índice $j(g)$ es el mismo para el producto de g con g_i y de g con σ_i porque numeramos los σ_i igual que los g_i, entonces poniendo

$$u = \prod_i h_i(g) \qquad \text{y} \qquad \tilde{u} = \prod_i \tilde{h}_i(g) \tag{1.6}$$

lo que debemos probar es que $u \equiv \tilde{u} \pmod{H'}$. Ahora, como $\sigma_i = g_ik_i$, para algún $k_i \in H$, entonces

$$g\sigma_i = gg_ik_i = g_{j(g)}h_i(g)k_i = g_{j(g)}k_{j(g)}k_{j(g)}^{-1}h_i(g)k_i = \sigma_{j(g)}k_{j(g)}^{-1}h_i(g)k_i \tag{1.7}$$

y así, de (1.7) y de la definición $g\sigma_i = \sigma_{j(g)}\tilde{h}_i(g)$ se sigue que

$$\tilde{h}_i(g) = k_{j(g)}^{-1}h_i(g)k_i, \qquad 1 \leq i \leq n \tag{1.8}$$

y de (1.6) y (1.8) se sigue que

$$\tilde{u} = \prod_i \tilde{h}_i(g) = \prod_i k_{j(g)}^{-1}h_i(g)k_i \equiv \prod_i h_i(g)k_{j(g)}^{-1}k_i \equiv u\left(\prod_i k_{j(g)}^{-1}\prod_i k_i\right) \pmod{H'}$$

donde la primer congruencia es porque H/H' es abeliano, y también notamos que $j(g)$ recorre $\mathbb{I}_n$ cuando i lo hace, por lo que los productos entre paréntesis en el lado derecho son inversos uno del otro, i.e., $\widetilde{u} \equiv u \pmod{H'}$ como se quería. □

Otra fórmula para el homomorfismo de transferencia. Si $g \in G$, consideremos el subgrupo cíclico $\langle g \rangle \subseteq G$. Se tiene una acción de $\langle g \rangle$ en el conjunto G/H de clases laterales izquierdas de H en G definida, para $g^i \in \langle g \rangle$ y $xH \in G/H$, por el producto $g^i xH$ y podemos considerar las órbitas de esta acción, i.e., para $xH \in G/H$ su órbita es

$$\mathrm{orb}_{\langle g \rangle}(xH) = \{xH, gxH, g^2xH, \ldots, g^{r_x-1}xH\}$$

donde r_x es el menor entero positivo tal que $g^{r_x}xH = xH$, i.e., $g^{r_x}x \equiv x \pmod{H}$. Consideremos todas las órbitas de esta acción, digamos

$$\mathrm{orb}_{\langle g \rangle}(x_1H), \mathrm{orb}_{\langle g \rangle}(x_2H), \ldots, \mathrm{orb}_{\langle g \rangle}(x_sH)$$

y en cada una de estas órbitas escojamos una clase x_iH y un elemento x_i en esta clase. Sea r_i el orden de la órbita de x_iH, i.e., el menor entero positivo tal que $g^{r_i}x_iH = x_iH$, i.e., $g^{r_i}x_i \equiv x_i \pmod{H}$. Como la unión de las órbitas es todo G/H y como las clases laterales en cada órbita son distintas, hemos mostrado que las clases de G/H tienen la forma $g^j x_i H$, para $1 \leq i \leq s$ y $0 \leq j \leq r_i - 1$, es decir, los elementos

$$(*) \qquad g^j x_i, \qquad 1 \leq i \leq s,\ 0 \leq j \leq r_i - 1$$

forman un conjunto completo de representantes de las clases en G/H y para calcular el homomorfismo de transferencia en términos de este conjunto de representantes, debemos escribir el producto $gg^j x_i$ en la forma th con $h \in H$ y t un representante en $(*)$. Ahora, el producto $g^{j+1}x_i$ es él mismo un representante (y por lo tanto $h = 1$ en este caso) excepto cuando $j = r_i - 1$, en cuyo caso

$$g^{j+1}x_i = g^{r_i}x_i \equiv x_i \pmod{H}$$

por definición de r_i (y así, $g^{r_i}x_i = x_i h$ con $h \in H$, por lo que $h = x_i^{-1}g^{r_i}x_i$ en este caso). Así, en el cálculo de $V(g)$ los únicos factores que no son necesariamente 1 son aquellos que corresponden a los productos $gg^{r_i-1}x_i$ para los cuales el h correspondiente es $h = x_i^{-1}g^{r_i}x_i$. Por lo que

$$V(g) = \prod_i x_i^{-1}g^{r_i}x_i \pmod{H'}$$

y ésta es la fórmula que usamos en la demostración del caso 2 en la nota 4. Note que si s es el número de órbitas de la acción de $\langle g \rangle$ en G/H y si $x_1, \ldots, x_s$ son representantes de estas órbitas, cada una de las cuales tiene longitud r_i, respectivamente, i.e.,

$$\mathrm{orb}_{\langle g \rangle}(x_iH) = \{x_iH, gx_iH, g^2x_iH, \ldots, g^{r_i-1}x_iH\}$$

y como estas órbitas forman una partición de G/H, entonces

$$\sum_{i=1}^{s} r_i = n = [G : H].$$

EJERCICIO 1. Si G es un grupo finito y χ es un carácter de G, definamos el conjunto

$$Z_\chi := \{g \in G \ : \ |\chi(g)| = \chi(1)\}.$$

Note que K_χ está contenido en Z_χ. Demuestre que Z_χ es un subgrupo de G. Note que, como $K_\chi \lhd G$, entonces se tendrá que $K_\chi \lhd Z_\chi$. *Sugerencia:* para demostrar que Z_χ es cerrado bajo productos, vea en la demostración del teorema 15.8,

$$|\chi(g)| = \chi(1) \Leftrightarrow \rho(g) : V \to V \text{ tiene un único valor propio, digamos } \lambda_g$$

y concluya que $\chi(gh) = \chi(1)\lambda_h\lambda_g$ (es la suma de los valores propios $\chi(1)$ veces).

EJERCICIO 2. Con la notación del ejercicio anterior, demuestre que si χ es irreducible, entonces $Z_\chi/K_\chi = Z(G/K_\chi)$ es el centro de G/K_χ.

EJERCICIO 3. Si χ_i son los caracteres irreducibles de G, escribiremos $Z_i := Z_{\chi_i}$. Si G es finito, no abeliano y simple, demuestre que $Z_i = 1$ para toda $i > 1$.

EJERCICIO 4. El centro de un grupo se puede leer de su tabla de caracteres: demuestre que $Z(G) = \bigcap_{i=1}^{r} Z_i$, donde $Z_i := Z_{\chi_i}$.

EJERCICIO 5. Las tablas de caracteres se pueden usar para decidir si un grupo es o no nilpotente. *Sugerencia*: Ejercicios 4 y 2.

EJERCICIO 6. Sea G un grupo de orden $p^r q^s$, con p, q primos y $r, s > 0$. Si $Z(G) = 1$, demuestre que existe un elemento $g \in G$, $g \neq 1$, tal que para su clase de conjugación C_g se tiene que $|C_g| \not\equiv 0 \pmod{q}$. Más aún, demuestre que $|C_g|$ es una potencia de p. *Sugerencia:* las clases de conjugación de los $\sigma \neq 1$ forman una partición de $G - \{1\}$

EJERCICIO 7. Usando el ejercicio anterior, dé otra demostración del teorema $p^r q^s$ de Burnside, distinguiendo dos casos: cuando $Z(G) \neq 1$ y cuando $Z(G) = 1$.

EJERCICIO 8. Sea χ el carácter de una representación irreducible y fiel de un grupo G. Demuestre que $Z(G) = \{g \in G \ : \ |\chi(g)| = \chi(1)\} = Z_\chi$.

EJERCICIO 9. Sea $\sigma \in G$ de orden k. Si σ es conjugado de σ^i, para todo i tal que $1 \leq i \leq k$ con $\text{mcd}(i, k) = 1$, demuestre que $\chi(\sigma) \in \mathbb{Z}$, para todos los caracteres χ de G.

EJERCICIO 10. Demuestre que todos los caracteres del grupo simétrico S_n tienen valores enteros. *Sugerencia*: ejercicio 23 del capítulo 4.

EJERCICIO 11. Bajo la correspondencia del lema 15.1 (vea también los ejercicios 15 y 16 del capítulo 13), si $N \lhd G$, los caracteres irreducibles de G/N corresponden a caracteres irreducibles χ de G tales que $N \subseteq \ker \chi$. Demuestre que $N = \bigcap K_\chi$, donde la intersección es sobre todos los caracteres irreducibles de G tales que $N \subseteq \ker \chi$. *Sugerencia*: Vea la demostración de la proposición 15.2.

EJERCICIO 12. La tabla de caracteres de un grupo finito G se puede usar para calcular el subgrupo conmutador de G. En efecto, demuestre que

$$[G : G] = \bigcap \{\ker \chi \ : \ \chi \text{ es un carácter irreducible de grado 1 de } G\}.$$

Sugerencia: Como $G/[G : G]$ es abeliano, todos sus caracteres irreducibles son de grado 1. Luego aplique el ejercicio anterior con $N = [G : G]$.

EJERCICIO 13. Uno puede leer de la tabla de caracteres de un grupo finito G los elementos que son conmutadores. En efecto, demuestre que un elemento $g \in G$ es un conmutador si y sólo si

$$\sum_{\chi \text{ irreducible}} \chi(g)/\chi(1) \neq 0,$$

donde la suma corre sobre todos los caracteres irreducibles de G.

EJERCICIO 14. Sean $K \subseteq H \subseteq G$ subgrupos de índice finito en G y sea ϕ un carácter de K. Si $\psi = \phi_K^H$ es el carácter de H inducido por ϕ, demuestre que $\phi_K^G = \psi_H^G = (\phi_K^H)_H^G$ (transitividad de la inducción).

EJERCICIO 15. Si G es un grupo de orden impar y si el número de clases de conjugación de G es k, demuestre que $|G| \equiv k \pmod{16}$.

EJERCICIO 16. Identifique el núcleo de Frobenius en D_8.

EJERCICIO 17. Si G es un grupo de Frobenius con complemento H y núcleo K, demuestre que $|H|$ divide a $|K| - 1$.

EJERCICIO 18. Si χ es un carácter irreducible de un grupo finito G, demuestre que $\overline{\chi}$ también es irreducible.

EJERCICIO 19. Sea M la tabla de caracteres de un grupo finito G, vista como una matriz cuadrada, y sea $\overline{M}$ la matriz que se obtiene de M tomando los conjugados complejos de sus entradas. Como para cada carácter irreducible χ que aparece en un renglón de M su conjugado $\overline{\chi}$ también aparece como otro renglón de M, demuestre que $\overline{M}$ se obtiene de M permutando sus renglones, i.e., $\overline{M} = PM$, donde P es una

matriz de permutaciones, i.e., P se obtiene de la matriz identidad I_n permutando sus renglones.

EJERCICIO 20. Similarmente, para cada clase de conjugación de un $g \in G$ consideremos su columna correspondiente en M y observe que también se tiene la columna correspondiente a la clase de conjugación de g^{-1} ya que $\chi(g^{-1}) = \overline{\chi}(g)$. Demuestre que $\overline{M}$ se obtiene de M permutando sus columnas, i.e., $\overline{M} = MQ$, con Q una matriz de permutaciones.

EJERCICIO 21. Una clase de conjugación C de un grupo finito G se dice que es *real* si para cada $g \in C$ se tiene que $g^{-1} \in C$. Por ejemplo, la clase de conjugación $\{1\}$ es real. Demuestre que el número de clases de conjugación reales de G es igual a $\mathrm{Tr}(Q)$, donde Q es la matriz de permutaciones del ejercicio anterior.

EJERCICIO 22. Demuestre que el número de caracteres irreducibles reales de G es igual a $\mathrm{Tr}(P)$, donde P es la matriz del ejercicio 19.

EJERCICIO 23. Concluya que si G es un grupo finito, el número de caracteres irreducibles reales de G es igual al número de clases de conjugación reales. *Sugerencia:* de los ejercicios 17 y 18 se tiene que $PM = MQ$, y por la ortogonalidad de caracteres M es invertible.

EJERCICIO 24. Usando el ejercicio anterior, demuestre que si un grupo finito no trivial G tiene un carácter irreducible no principal real, entonces $|G|$ es par.

Apéndice A

Enteros algebraicos

En este apéndice recolectamos algunas definiciones y resultados elementales sobre enteros algebraicos, que usamos en la demostración del teorema $p^a q^b$ de Burnside y en el hecho de que el grado de un carácter irreducible de un grupo finito, divide al orden del grupo. El enfoque que hemos elegido usa polinomios simétricos en algunos puntos importantes, como se estilizaba hace algún tiempo, pero es un punto de vista que enlaza armónicamente con el tema, en el sentido musical, que permea este libro, a saber, el estudio de los objetos que permanecen invariantes bajo la acción de un grupo, en este caso concreto, los polinomios (en un número finito de indeterminadas) que son invariantes bajo la acción natural del grupo simétrico que permuta a estas indeterminadas.

Polinomios simétricos. Sea $K[x_1, \ldots, x_n]$ el anillo de polinomios en n variables con coeficientes en un campo $K \subseteq \mathbb{C}$ y sea S_n el grupo simétrico en n letras. Se tiene una acción natural del grupo S_n en $K[x_1, \ldots, x_n]$ dada como sigue: para cada permutación $\sigma \in S_n$ y cualquier polinomio $f(x_1, \ldots, x_n) \in K[x_1, \ldots, x_n]$, se define el polinomio f^σ permutando las variables x_i de acuerdo a σ, es decir,

$$f^\sigma(x_1, \ldots, x_n) := f(x_{\sigma(1)}, \ldots, x_{\sigma(n)}).$$

El polinomio f se dice que es *simétrico* si $f^\sigma = f$ para toda $\sigma \in S_n$.

Ejemplo 4. El origen de los polinomios simétricos es el siguiente: si $\alpha_1, \ldots, \alpha_n$ son todas las raíces de un polinomio en una variable

$$f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = (x - \alpha_1) \cdots (x - \alpha_n) = \prod_{i=1}^{n} (x - \alpha_i),$$

entonces los coeficientes a_k de $f(x)$ se pueden escribir en términos de las raíces α_i mediante las fórmulas de Viète:

$$
\begin{aligned}
a_{n-1} &= (-1)^1 \sum_{i=1}^{n} \alpha_i \\
a_{n-2} &= (-1)^2 \sum_{1 \le i < j \le n} \alpha_i \alpha_j \\
a_{n-3} &= (-1)^3 \sum_{1 \le i < j < k \le n} \alpha_i \alpha_j \alpha_k \\
&\vdots \\
a_0 &= (-1)^n \alpha_1 \alpha_2 \cdots \alpha_n,
\end{aligned}
$$

donde en la derecha aparecen las sumas de productos de k factores ordenados, $1 \le k \le n$, de las raíces $\alpha_1, \ldots, \alpha_n$, a las cuales se suele denotar por

$$
s_k(\alpha_1, \ldots, \alpha_n) := \sum_{1 \le i_1 < \cdots < i_k \le n} \alpha_{i_1} \cdots \alpha_{i_k}
$$

y los s_k se llaman los *polinomios simétricos elementales* de grado k en los $\alpha_1, \ldots, \alpha_n$. Así, las fórmulas anteriores se escriben

$$
\begin{aligned}
a_{n-1} &= (-1)^1 s_1(\alpha_1, \ldots, \alpha_n) \\
a_{n-2} &= (-1)^2 s_2(\alpha_1, \ldots, \alpha_n) \\
a_{n-3} &= (-1)^3 s_3(\alpha_1, \ldots, \alpha_n) \\
&\vdots \\
a_0 &= (-1)^n s_n(\alpha_1, \ldots, \alpha_n)
\end{aligned}
$$

y la validez de estas fórmulas es el contenido del teorema siguiente:

TEOREMA A.1 (Fórmulas de Viète). *Sea $f(x) \in K[x]$ un polinomio mónico de grado n:*

$$
f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0
$$

con raíces $\alpha_1, \ldots, \alpha_n$, repetidas de acuerdo a su multiplicidad. Entonces, los coeficientes a_i de $f(x)$ y sus raíces α_j se relacionan mediante las fórmulas

$$
a_i = (-1)^{n-i} s_{n-i}(\alpha_1, \ldots, \alpha_n),
$$

donde los $s_k(\alpha_1, \ldots, \alpha_n)$ son los polinomios simétricos elementales.

Demostración. Por inducción sobre n observando que los casos iniciales $n = 1$ y $n = 2$ son directos. Supongamos que el resultado es válido para polinomios de grado $< n$ y escribamos

$$
f(x) = g(x)(x - \alpha_n) \quad \text{con } g(x) = x^{n-1} + b_{n-2}x^{n-2} + \cdots + b_1 x + b_0
$$

donde observamos que las raíces de $g(x)$ son $\alpha_1, \ldots, \alpha_{n-1}$ y satisfacen, por hipótesis de inducción las fórmulas de Viète:

$$b_j = (-1)^{n-1-j} s_{n-1-j}(\alpha_1, \ldots, \alpha_{n-1}).$$

Ahora, de la igualdad $f(x) = g(x)(x - \alpha_n)$ se obtiene

$$\begin{aligned} x^n + a_{n-1}x^{n-1} + \cdots + a_0 &= (x^{n-1} + b_{n-2}x^{n-2} + \cdots + b_1 x + b_0)(x - \alpha_n) \\ &= x^n + (b_{n-2} - \alpha_n)x^{n-1} + (b_{n-3} - \alpha_n b_{n-2})x^{n-2} \\ &\quad + \cdots + (b_0 - \alpha_n b_1)x - \alpha_n b_0, \end{aligned}$$

e igualando coeficientes obtenemos

$$\begin{aligned} a_{n-1} &= b_{n-2} - \alpha_n = (-1)^1 s_1(\alpha_1, \ldots, \alpha_{n-1}) - \alpha_n = -s_1(\alpha_1, \ldots, \alpha_n) \\ a_{n-2} &= b_{n-3} - \alpha_n b_{n-2} = (-1)^2 s_2(\alpha_1, \ldots, \alpha_{n-1}) - \alpha_n(-1)s_1(\alpha_1, \ldots, \alpha_{n-1}) \\ &= s_2(\alpha_1, \ldots, \alpha_{n-1}) + \alpha_n s_1(\alpha_1, \ldots, \alpha_{n-1}) \\ a_{n-3} &= b_{n-4} - \alpha_n b_{n-3} = (-1)^3 s_3(\alpha_1, \ldots, \alpha_{n-1}) - \alpha_n(-1)^2 s_2(\alpha_1, \ldots, \alpha_{n-1}) \\ &= (-1)^3[s_3(\alpha_1, \ldots, \alpha_{n-1}) + \alpha_n s_2(\alpha_1, \ldots, \alpha_{n-1})] \end{aligned}$$

y, en general,

$$(*) \qquad a_{n-k} = (-1)^k[s_k(\alpha_1, \ldots, \alpha_{n-1}) + \alpha_n s_{k-1}(\alpha_1, \ldots, \alpha_{n-1})]$$

donde observamos que

$$(\dagger) \qquad s_k(\alpha_1, \ldots, \alpha_n) = s_k(\alpha_1, \ldots, \alpha_{n-1}) + \alpha_n s_{k-1}(\alpha_1, \ldots, \alpha_{n-1})$$

para $1 \leq k \leq n-1$ (separarando, en la definición del polinomio $s_k(\alpha_1, \ldots, \alpha_n)$ los sumandos que no contienen a α_n y los que sí lo contienen). De esta observación y de $(*)$ se sigue que

$$a_{n-k} = (-1)^k s_k(\alpha_1, \ldots, \alpha_n),$$

que es lo que se quería probar, poniendo $i = n - k$. □

Para probar que los polinomios simétricos elementales $s_k(x_1, \ldots, x_n)$ son, en efecto, simétricos, escribiremos a los polinomios s_k en una forma que se presta para hacer ésto: denotemos con $\mathbb{S}_k$ a la familia de todos los subconjuntos de $\mathbb{I}_n$ con k elementos y observe que cada $Y \in \mathbb{S}_k$ se puede escribir, en forma única, como $Y = \{i_1, \ldots, i_k\}$ con $1 \leq i_1 < \cdots < i_k \leq n$, y se tiene que

$$(*) \qquad s_k = s_k(x_1, \ldots, x_n) = \sum_{Y \in \mathbb{S}_k} \left(\prod_{i \in Y} x_i \right).$$

Ahora, cada $\sigma \in S_n$ induce una permutación de los elementos de $\mathbb{S}_k$ mediante

$$\sigma(Y) = \sigma\{i_1, \ldots, i_k\} = \{\sigma(i_1), \ldots, \sigma(i_k)\} =: Y'$$

donde $Y' \in \mathbb{S}_k$ porque Y' tiene k elementos ya que σ es inyectiva. También, si $Y' = \{i'_1, \ldots, i'_k\} \in \mathbb{S}_k$ es cualquier conjunto con k elementos, entonces el conjunto $Y = \{\sigma^{-1}(i'_1), \ldots, \sigma^{-1}(i'_k)\} \in \mathbb{S}_k$ es tal que $\sigma Y = Y'$. En otras palabras, la acción de S_n en $\mathbb{S}_k$ es *transitiva*. Sin embargo note que esta acción no tiene por qué preservar el orden de los elementos de un $Y \in \mathbb{S}_k$ dado.

Con las observaciones anteriores es fácil probar que los polinomios s_k son simétricos, ya que si $\sigma \in S_n$,

$$\begin{aligned} s_k^{\sigma}(x_1, \ldots, x_n) &= \Big(\sum_{Y \in \mathbb{S}_k} \Big(\prod_{i \in Y} x_i \Big) \Big)^{\sigma} \quad \text{por } (*) \\ &= \sum_{Y \in \mathbb{S}_k} \Big(\prod_{i \in Y} x_{\sigma(i)} \Big) \\ &= \sum_{Y \in \mathbb{S}_k} \Big(\prod_{i' \in \sigma Y} x_{i'} \Big) \\ &= \sum_{Y' \in \mathbb{S}_k} \Big(\prod_{i' \in Y'} x_{i'} \Big) \quad \text{con } Y' = \sigma Y \\ &= s_k(x_1, \ldots, x_n) \end{aligned}$$

(la última igualdad por $(*)$, ya que Y' recorre $\mathbb{S}_k$ cuando Y lo hace.) □

Como la acción de S_n en $K[x_1, \ldots, x_n]$ es lineal, con los polinomios simétricos elementales s_k podemos formar más ejemplos de polinomios simétricos:

(1) Si $s = s_i + s_j$ es una suma de polinomios simétricos elementales, entonces s también es simétrico.

(2) Si $s = s_i s_j$ es un producto de polinomios simétricos elementales, entonces s también es simétrico.

(3) Si $s = \lambda s_i$, con $\lambda \in K$, entonces s también es simétrico.

(4) Se sigue que, si $h \in K[x_1, \ldots, x_n]$ se puede escribir como un polinomio en los polinomios simétricos elementales $s_1, \ldots, s_n$, entonces h también es simétrico.

La afirmación recíproca de (4) también es cierta y para probarla usaremos la noción de componente homogénea de un polinomio: dado un polinomio $f(x_1, \ldots, x_n)$ en n variables con coeficientes en K podemos escribir a f como

$$f(x_1, \ldots, x_n) = \sum_I a_I x_1^{d_1} \cdots x_n^{d_n}$$

donde $I = (d_1, \ldots, d_n)$ y decimos que $x_1^{d_1} \cdots x_n^{d_n}$ es un *monomio* de grado $d_1 + \cdots + d_n$. Si juntamos todos los monomios en f de un mismo grado, digamos d, llamaremos

al polinomio correspondiente la *componente homogénea de grado d* de f. Por ejemplo, si

$$f(x_1, x_2) = 6 + 3x_1 + 4x_2 + 3x_1^2 - 2x_1x_2 - 7x_2^3$$

la componente homogénea de grado 2 es $3x_1^2 - 2x_1x_2$, la componente homogénea de grado 3 es $-7x_2^3$, la componente homogénea de grado 1 es $3x_1 + 4x_2$ y la componente homogénea de grado 0 es el término independiente 6. Todo polinomio f se puede separar en una suma de sus componentes homogéneas y diremos que f es un polinomio homogéneo si sólo tiene una componente homogénea.

TEOREMA A.2. *Un polinomio $h \in K[x_1, \ldots, x_n]$ es simétrico si y sólo si h se puede expresar como un polinomio, con coeficientes en K, en los polinomios simétricos elementales $s_1, \ldots, s_n$.*

Demostración. Para la implicación faltante, la idea es reducir un polinomio simétrico arbitario h en sumas de productos de polinomios simétricos elementales. Para ésto, primero ordenamos los monomios $x_1^{e_1} \cdots x_n^{e_n}$ lexicográficamente, estipulando que

$$x_1^{a_1} \cdots x_n^{a_n} \prec x_1^{b_1} \cdots x_n^{b_n}$$

si la primera diferencia $b_i - a_i$ no nula es positiva. Por ejemplo, $x_1x_2^2 \prec x_1^2x_2$.

Note ahora que la acción del grupo simétrico S_n en $K[x_1, \ldots, x_n]$ manda polinomios homogéneos en polinomios homogéneos del mismo grado. Se sigue que, un polinomio h es simétrico si y sólo si cada una de sus componentes homogéneas lo es. Entonces, sin perder generalidad, podemos suponer que h es homogéneo simétrico.

Procedemos ahora por inducción usando el orden lexicográfico: supongamos que $x_1^{a_1} \cdots x_n^{a_n}$ es el mayor monomio de h con coeficiente a no nulo. Entonces, $a_{i+1} \leq a_i$ para todo i, ya que si éste no fuera el caso, existiría un i menor tal que $a_{i+1} > a_i$. Pero entonces la transposición $\tau = (i, i+1) \in S_n$ aplicada a h (que satisface que $h^\tau = h$) implicaría que el monomio

$$x_1^{a_1} \cdots x_i^{a_{i+1}} x_{i+1}^{a_i} \cdots x_n^{a_n}$$

también aparece en h con coeficiente a; pero este monomio es mayor, en el orden lexicográfico, que $x_1^{a_1} \cdots x_n^{a_n}$, lo cual es una contradicción con la elección de este monomio. Se sigue que $a_{i+1} \leq a_i$ para toda i, y por lo tanto cada uno de los exponentes del producto siguiente es ≥ 0 (y así el resultado es un polinomio):

$$s_1^{a_1 - a_2} s_2^{a_2 - a_3} \cdots s_{n-1}^{a_{n-1} - a_n} s_n^{a_n}$$

y observe que el monomio mayor del producto anterior también es $x_1^{a_1} \cdots x_n^{a_n}$. Entonces,

$$g := h - a s_1^{a_1 - a_2} s_2^{a_2 - a_3} \cdots s_{n-1}^{a_{n-1} - a_n} s_n^{a_n}$$

es un polinomio simétrico cuyo monomio mayor es más chico que el monomio mayor de h y además g es simétrico. Por hipótesis de inducción g se puede expresar como un

polinomio en los polinomios simétricos elementales y despejando a h de la igualdad anterior se obtiene el resultado deseado. □

El resultado siguiente se usará en la sección de conjugados algebraicos, para mostrar que cierto polinomio tiene coeficientes racionales:

COROLARIO A.3. *Si $p(x) \in \mathbb{Q}[x]$ es un polinomio mónico de grado n con raíces $\xi_1, \ldots, \xi_n$ y si $h(x_1, \ldots, x_n) \in \mathbb{Q}[x_1, \ldots, x_n]$ es simétrico, entonces $h(\xi_1, \ldots, \xi_n) \in \mathbb{Q}$.*

Demostración. Por las fórmulas de Viète los coeficientes $a_k \in \mathbb{Q}$ de $p(x)$ se pueden expresar como los polinomios simétricos elementales en las raíces $\xi_1, \ldots, \xi_k$ y por lo tanto cada $s_k(\xi_1, \ldots, \xi_n) = \pm a_k \in \mathbb{Q}$. Por el teorema previo, $h(\xi_1, \ldots, \xi_n)$ es un polinomio, con coeficientes en $\mathbb{Q}$, en los $s_k(\xi_1, \ldots, \xi_n) \in \mathbb{Q}$ y por lo tanto $h(\xi_1, \ldots, \xi_n) \in \mathbb{Q}$. □

Números algebraicos. Un número complejo $\alpha \in \mathbb{C}$ se dice que es *algebraico* si existe un polinomio no nulo

$$p(x) = a_0 + a_1 x + \cdots + a_{n-1}x^{n-1} + a_n x^n \in \mathbb{Q}[x]$$

tal que $p(\alpha) = 0$. Si ahora dividimos $p(x)$ por $a_n \neq 0$, se obtiene un polinomio

$$q(x) = x^n + b_{n-1}x^{n-1} + \cdots + b_1 x + b_0 \in \mathbb{Q}[x]$$

con $b_j = a_j/a_n \in \mathbb{Q}$, y claramente $q(\alpha) = 0$. Así, si $\alpha \in \mathbb{C}$ es algebraico, entonces α es raíz de un polinomio no constante en $\mathbb{Q}[x]$ cuyo coeficiente de grado es 1. A un polinomio cuyo coeficiente de grado es 1 se le llama *mónico* y diremos que el polinomio $q(x)$ de arriba es el polinomio mónico obtenido a partir de $p(x)$. Por el principio del buen orden en $\mathbb{N}$, si $\alpha \in \mathbb{C}$ es algebraico, del conjunto de polinomios mónicos de $\mathbb{Q}[x]$ de los cuales α es raíz, existe uno de menor grado. Denotemos a este polinomio por $m(x) \in \mathbb{Q}[x]$.

LEMA A.4. *El polinomio mónico de menor grado $m(x) \in \mathbb{Q}[x]$ del cual $\alpha \in \mathbb{C}$ es raíz, es único. Más aún, $m(x)$ es irreducible en $\mathbb{Q}[x]$, y $m(x)$ divide a cualquier otro polinomio $p(x) \in \mathbb{Q}[x]$ del cual α es raíz.*

Demostración. Si $m(x)$, $f(x) \in \mathbb{Q}[x]$ son mónicos de menor grado tal que $m(\alpha) = 0 = f(\alpha)$, entonces sea $n = \text{gr}(m) = \text{gr}(f)$. Así, para $h(x) := m(x) - f(x) \in \mathbb{Q}[x]$, se tiene que $h(\alpha) = 0$, y si $h(x) \neq 0$, $\text{gr}(h) < n$. Entonces, si $\tilde{h}(x)$ es el mónico obtenido a partir de $h(x)$, $\tilde{h}(\alpha) = 0$ con $\text{gr}(\tilde{h}) = \text{gr}(h) < n$, una contradicción con la minimalidad del grado de $m(x)$ y $f(x)$. Se sigue que $h(x) = 0$ y así $m(x) = f(x)$.

Ahora, si sucediera que $m(x) = p(x) \cdot q(x)$ en $\mathbb{Q}[x]$, con $\text{gr}(p) < \text{gr}(m)$, $\text{gr}(q) < \text{gr}(m)$, entonces se pueden escoger p y q mónicos, y como $0 = m(\alpha) = p(\alpha) \cdot q(\alpha)$, entonces α sería raíz de $p(x)$ ó de $q(x)$, ambos de grado menor que $m(x)$, una contradicción. Así, $m(x)$ es irreducible.

Finalmente, si $\phi(x) \in \mathbb{Q}[x]$ es tal que $\phi(\alpha) = 0$, dividiendo entre $m(x)$ se tiene que:

$$\phi(x) = m(x)q(x) + r(x)$$

con $r(x) = 0$ ó $\text{gr}(r) < \text{gr}(\phi)$. Pero como

$$0 = \phi(\alpha) = m(\alpha)q(\alpha) + r(\alpha) = 0 + r(\alpha) = r(\alpha)$$

entonces, por la minimalidad del grado de $m(x)$, no se puede tener que $r \neq 0$. Se sigue que $r(x) = 0$ y en consecuencia $m(x)|\phi(x)$. □

Al polinomio mónico, irreducible $m(x) \in \mathbb{Q}[x]$ y de grado menor del cual $\alpha \in \mathbb{C}$ es raíz, se le llama el *polinomio mínimo* (irreducible) de α, y se denota $m(x) = \text{Irr}(\alpha, \mathbb{Q})$.

Si $\alpha \in \mathbb{C}$ es un número algebraico y si $f(x)$ es cualquier polinomio en $\mathbb{Q}[x]$, entonces $f(\alpha)$ es un número complejo. Ahora, si $g(x) \in \mathbb{Q}[x]$ es tal que $g(\alpha) \neq 0$, entonces $f(\alpha)/g(\alpha)$ es un número complejo y podemos entonces considerar al conjunto de números complejos de esa forma

$$\mathbb{Q}(\alpha) := \left\{ \frac{p(\alpha)}{q(\alpha)} : p(x), q(x) \in \mathbb{Q}[x], \quad q(\alpha) \neq 0 \right\}.$$

Se demuestra fácilmente que, con las operacions de $\mathbb{C}$, el conjunto $\mathbb{Q}(\alpha)$ es cerrado bajo sumas, productos, restas y si $f(\alpha)/g(\alpha) \neq 0$, entonces $f(\alpha) \neq 0$ y $g(\alpha)/f(\alpha) \in \mathbb{Q}(\alpha)$ es el inverso multiplicativo de $f(\alpha)/g(\alpha)$. En otras palabras, $\mathbb{Q}(\alpha)$ es un *campo*, y decimos que se obtiene *adjuntando* α a $\mathbb{Q}$. También decimos que es una *extensión simple*. Observe que este campo contiene a $\mathbb{Q}$, porque si $r \in \mathbb{Q}$, entonces $r = r/1 = f(r)/1$ donde $f(x) = x$ y $g(x) = 1$ (constante). La inclusion $\mathbb{Q} \subseteq \mathbb{Q}(\alpha)$ se llama una *extensión de campos* y se denota por $\mathbb{Q}(\alpha)/\mathbb{Q}$. Observe que esta inclusión implica que el campo $\mathbb{Q}(\alpha)$ es un espacio vectorial sobre $\mathbb{Q}$ por lo que podemos considerar su dimensión. El teorema A.6 dice que cuando α es un número algebraico, esta dimensión es *finita* y la proposición A.5 dice que cuando α es algebraico, el campo $\mathbb{Q}(\alpha)$ tiene una descripción sencilla:

PROPOSICIÓN A.5. *Sea $\alpha \in \mathbb{C}$ algebraico y sea $m(x) = \text{Irr}(\alpha, \mathbb{Q}) \in \mathbb{Q}[x]$. Entonces,*

$$\mathbb{Q}(\alpha) = \{p(\alpha) : p(x) \in \mathbb{Q}[x] \text{ y } \text{gr}(p(x)) < \text{gr}(m(x))\}.$$

Demostración. Sea $\beta = p(\alpha)/q(\alpha) \in \mathbb{Q}(\alpha)$, $q(\alpha) \neq 0$. Como $q(\alpha) \neq 0$ entonces $m(x) \nmid q(x)$ y como $m(x)$ es irreducible entonces $\text{mcd}(m(x), q(x)) = 1$ y así existen $a(x), b(x)$ en $\mathbb{Q}[x]$ tales que $1 = m(x) \cdot a(x) + q(x) \cdot b(x)$ y así

$$1 = m(\alpha)a(\alpha) + q(\alpha)b(\alpha) = q(\alpha)b(\alpha),$$

es decir, $b(\alpha) = 1/q(\alpha)$, y por lo tanto

$$\beta = \frac{p(\alpha)}{q(\alpha)} = p(\alpha) \cdot b(\alpha) = h(\alpha)$$

donde $h(x) = p(x)b(x) \in \mathbb{Q}[x]$. Ahora, $h(x)$ se puede elegir de grado menor que el de $m(x)$, ya que si no es así, dividiendo

$$h(x) = m(x) \cdot A(x) + R(x) \text{ en } \mathbb{Q}[x]$$

con $\text{gr}(R) < \text{gr}(m)$, y $h(\alpha) = m(\alpha)A(\alpha) + R(\alpha) = R(\alpha)$, i.e. $\beta = h(\alpha) = R(\alpha)$ con $\text{gr}(R) < \text{gr}(m)$. Nótese que $R(x) \neq 0$ ya que si no fuera así se tendría que $h(x) = m(x)A(x)$, i.e., $0 = h(\alpha) = \beta \neq 0$, una contradicción. □

El resultado siguiente nos da un criterio importante para la algebricidad de un $\alpha \in \mathbb{C}$:

TEOREMA A.6. *Un $\alpha \in \mathbb{C}$ es algebraico si y sólo si la extensión $\mathbb{Q}(\alpha)/\mathbb{Q}$ tiene dimensión finita.*

Demostración. (1) Supongamos que $\mathbb{Q}(\alpha)/\mathbb{Q}$ es de dimensión finita n. Los $n+1$ elementos $1, \alpha, \alpha^2, \ldots, \alpha^n$ están en $\mathbb{Q}(\alpha)$ y como $\dim_{\mathbb{Q}} \mathbb{Q}(\alpha) = n$, entonces son linealmente dependientes sobre $\mathbb{Q}$, i.e., existen $a_0, a_1, \ldots, a_n \in \mathbb{Q}$ *no todos cero* tales que $a_0 + a_1\alpha + \cdots + a_n\alpha^n = 0$, i.e., α satisface al polinomio no constante

$$p(x) = a_0 + a_1 x + \cdots + a_n x^n \in \mathbb{Q}[x],$$

i.e., α es algebraico.

(2) Recíprocamente, si $\alpha \in \mathbb{C}$ es algebraico, sea $m(x) = \text{Irr}(\alpha, \mathbb{Q}) \in \mathbb{Q}[x]$ el polinomio mínimo de α. Sea $n = \text{gr}(m(x))$. Mostraremos que

$$\dim_{\mathbb{Q}} \mathbb{Q}(\alpha) = \text{gr}(\text{Irr}(\alpha, \mathbb{Q})) = \text{gr}(m(x)) = n.$$

En efecto, como $\mathbb{Q}(\alpha) = \{p(\alpha) : p(x) \in \mathbb{Q}[x], \text{gr}(p) < \text{gr}(m)\}$, una base de $\mathbb{Q}(\alpha)$ sobre $\mathbb{Q}$ está dada por $1, \alpha, \alpha^2, \ldots, \alpha^{n-1} \in \mathbb{Q}(\alpha)$, ya que,

(i) *Genera:* Si $\beta = p(\alpha) \in \mathbb{Q}(\alpha)$, $\beta = b_0 + b_1\alpha + \cdots + b_m\alpha^m$ con $m < n$.

(ii) *Es linealmente independiente:* Si $a_0 \cdot 1 + a_1 \cdot \alpha + \cdots + a_{n-1} \cdot \alpha^{n-1} = 0$ con $a_j \in \mathbb{Q}$, entonces para $p(x) = a_0 + a_1 x + \cdots + a_{n-1}x^{n-1} \in \mathbb{Q}[x]$ se tendría que $p(\alpha) = 0$ con $\text{gr}(p) < \text{gr}(m)$ en contradicción con la minimalidad del grado de $m(x)$, a menos que todos los $a_j = 0$. □

COROLARIO A.7. *Si $\alpha \in \mathbb{C}$ es algebraico, entonces* $\dim_{\mathbb{Q}} \mathbb{Q}(\alpha) = \text{gr}(\text{Irr}(\alpha, \mathbb{Q}))$.

□

Ejemplo 1. $\sqrt{2} \in \mathbb{R}$ es algebraico y de hecho $\text{Irr}(\sqrt{2}, \mathbb{Q}) = x^2 - 2 \in \mathbb{Q}[x]$, por lo que

$$\dim_{\mathbb{Q}} \mathbb{Q}(\sqrt{2}) = \text{gr}(x^2 - 2) = 2 \qquad \text{y} \qquad \mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}.$$

Ejemplo 2. Para $i \in \mathbb{C}$, $i^2 = -1$, se tiene que $\mathrm{Irr}(i, \mathbb{R}) = x^2 + 1 \in \mathbb{R}[x]$ por lo que

$$\mathbb{R}(i) = \{a + bi : a, b \in \mathbb{R}\} = \mathbb{C} \qquad \text{y} \qquad \dim_{\mathbb{R}} \mathbb{R}(i) = \dim_{\mathbb{R}} \mathbb{C} = 2.$$

Ejemplo 3. Para $\sqrt[3]{2} \in \mathbb{R}$, $\mathrm{Irr}(\sqrt[3]{2}, \mathbb{Q}) = x^3 - 2$ y $\dim_{\mathbb{Q}} \mathbb{Q}(\sqrt[3]{2}) = 3$, y de hecho

$$\mathbb{Q}(\sqrt[3]{2}) = \{a + b\sqrt[3]{2} + c(\sqrt[3]{2})^2 : a, b, c \in \mathbb{Q}\}.$$

COROLARIO A.8. *Si α es algebraico, entonces todos los elementos de $\mathbb{Q}(\alpha)$ son algebraicos.*

Demostración. Por el corolario anterior, $\mathbb{Q}(\alpha)/\mathbb{Q}$ tiene dimensión finita n. Si $\beta \in \mathbb{Q}(\alpha)$ es arbitrario, entonces los $n + 1$ elementos $1, \beta, \beta^2, \ldots, \beta^n \in \mathbb{Q}(\alpha)$ son linealmente dependientes y así existen $a_0, a_1, \ldots, a_n \in \mathbb{Q}$ no todos cero tales que

$$a_0 \cdot 1 + a_1\beta + \cdots + a_n\beta^n = 0$$

i.e., β es raíz del polinomio no cero $p(x) = a_0 + a_1x + \cdots + a_nx^n \in \mathbb{Q}[x]$. □

Hasta ahora hemos considerado extensiones simples $\mathbb{Q}(\alpha)/\mathbb{Q}$ y como $\mathbb{Q}(\alpha)$ es un campo contenido en $\mathbb{C}$, dado otro número complejo $\beta \in \mathbb{C}$, podemos adjuntar β a $\mathbb{Q}(\alpha)$, i.e., podemos considerar el conjunto

$$\mathbb{Q}(\alpha)(\beta) := \left\{ \frac{f(\beta)}{g(\beta)} \ : \ f(x), g(x) \in \mathbb{Q}(\alpha)[x] \ \text{ con } \ g(\beta) \neq 0 \right\}$$

y es fácil de demostrar que con las operaciones de $\mathbb{C}$ el conjunto $\mathbb{Q}(\alpha)(\beta)$ es un campo. También es claro que $\mathbb{Q}(\alpha)(\beta)$ contiene al campo $\mathbb{Q}(\alpha)$. Para simplificar la notación, denotaremos à $\mathbb{Q}(\alpha)(\beta)$ como $\mathbb{Q}(\alpha, \beta)$. Se tiene así una extensión $\mathbb{Q}(\alpha, \beta)/\mathbb{Q}$ la cual decimos que se obtiene adjuntando α y β a $\mathbb{Q}$. Podemos iterar esta construcción adjuntando un número finito de complejos a $\mathbb{Q}$. Sin embargo, el resultado siguiente nos dice que todas las extensiones de la forma $\mathbb{Q}(\alpha_1, \ldots, \alpha_n)$ con los $\alpha_i \in \mathbb{C}$ algebraicos, son simples, donde por un argumento inductivo se ve que es suficiente probar el resultado para $n = 2$:

TEOREMA A.9. *Si $\alpha, \beta \in \mathbb{C}$ son algebraicos, entonces existe un elemento $\theta \in \mathbb{Q}(\alpha, \beta)$ tal que $\mathbb{Q}(\alpha, \beta) = \mathbb{Q}(\theta)$.*

Demostración. Sean $p(x) = \mathrm{Irr}(\alpha, \mathbb{Q})$ y $q(x) = \mathrm{Irr}(\beta, \mathbb{Q})$ de grados m y n, respectivamente. Sean $\alpha = \alpha_1, \ldots, \alpha_m$ y $\beta = \beta_1, \ldots, \beta_n$ todas las raíces (distintas) de $p(x)$ y $q(x)$, respectivamente. Pongamos

$$K = \mathbb{Q}(\alpha_1, \ldots, \alpha_m, \beta_1, \ldots, \beta_n).$$

Observe ahora que si $j \neq 1$, entonces $\beta_j \neq \beta$, por lo que la ecuación

$$(*) \qquad \alpha_i + X\beta_j = \alpha + X\beta$$

tiene una única solución en K, a saber,

$$X = \frac{\alpha_i - \alpha}{\beta - \beta_j}$$

y como $\mathbb{Q} \subseteq K$, entonces $(*)$ tiene a lo más una solución en $\mathbb{Q}$. Ahora, como sólo hay un número finito de ecuaciones $(*)$, entonces sólo hay un número finito de elementos de $\mathbb{Q}$ que satisfacen $(*)$ y como $\mathbb{Q}$ tiene un número infinito de elementos, podemos encontrar un $r \in \mathbb{Q}$, $r \neq 0$, que no es ninguna de las soluciones de las ecuaciones $(*)$, i.e., tal que

$$\alpha_i + r\beta_j \neq \alpha + r\beta \quad \text{para toda } i \text{ y para toda } j \neq 1. \tag{1}$$

Pongamos

$$\theta := \alpha + r\beta \in \mathbb{Q}(\alpha, \beta). \tag{2}$$

Mostraremos que $\mathbb{Q}(\theta) = \mathbb{Q}(\alpha, \beta)$. Observe primero que, como $\theta \in \mathbb{Q}(\alpha, \beta)$ por (2), entonces $\mathbb{Q}(\theta) \subseteq \mathbb{Q}(\alpha, \beta)$. Para la otra inclusión, basta probar que $\alpha, \beta \in \mathbb{Q}(\theta)$. Para ésto, pongamos $h(x) := p(\theta - rx) \in \mathbb{Q}(\theta)[x]$; entonces, como α es raíz de $p(x)$,

$$h(\beta) = p(\theta - r\beta) = p(\alpha) = 0 \quad \text{ya que } \alpha = \theta - r\beta \text{ por (2)},$$

y como β es raíz de $q(x) \in \mathbb{Q}[x] \subseteq \mathbb{Q}(\theta)[x]$, entonces $h(x)$ y $q(x)$ tienen el cero común β, i.e., tienen el factor común $x - \beta$ como polinomios en $\mathbb{C}[x]$. Mostraremos que

$$\operatorname{mcd}(h, q) = x - \beta.$$

En efecto, si $\beta_j \neq \beta$ es otra raíz de $q(x)$, entonces $h(\beta_j) = p(\theta - r\beta_j) \neq 0$ ya que, por la elección de $r \in \mathbb{Q}$, según (1) y (2) se tiene que

$$\theta - r\beta_j = \alpha + r\beta - r\beta_j \neq \alpha_i + r\beta_j - r\beta_j = \alpha_i,$$

i.e., $\theta - r\beta_j \neq \alpha_i$, para $j \neq 1$, i.e., $\theta - r\beta_j$ no es ninguna de las raíces de $p(x)$ para $j \neq 1$. Así, ninguno de los otros $x - \beta_j$, con $j \neq 1$, es factor de $h(x)$. Además, como $(x-\beta)^2 \nmid q(x)$ (ya que las raíces de $q(x)$ son distintas), entonces $(x-\beta)^2 \nmid \operatorname{mcd}(h, q)$. Se sigue que $x - \beta$ es el mcd de h y q, que son polinomios en $\mathbb{Q}(\theta)[x]$. Por lo tanto $x - \beta$ es combinación lineal de h y q, i.e., existen polinomios $s(x), t(x) \in \mathbb{Q}(\theta)[x]$ tales que

$$x - \beta = h(x)s(x) + q(x)t(x)$$

donde el lado derecho es un polinomio con coeficientes en $\mathbb{Q}(\theta)$. Se sigue que $\beta \in \mathbb{Q}(\theta)$. Finalmente, se tiene que $\alpha = \theta - r\beta \in \mathbb{Q}(\theta)$ y así $\alpha \in \mathbb{Q}(\theta)$. □

Conjugados algebraicos. Si $\alpha \in \mathbb{C}$ es un número algebraico y si $\phi(x) = \operatorname{Irr}(\alpha, \mathbb{Q})$, a las raíces $\alpha = \alpha_1, \ldots, \alpha_m$ de $\phi(x)$ se les llama los *conjugados algebraicos* de α. Note

que como son raíces de $\phi(x)$, los α_i también son números algebraicos. Adjuntando estas raíces a $\mathbb{Q}$ obtenemos el campo

$$K = \mathbb{Q}(\alpha_1, \ldots, \alpha_m)$$

y por el teorema A.9 existe un elemento $\theta \in \mathbb{C}$ tal que $K = \mathbb{Q}(\theta)$. Sea $p(x) = \text{Irr}(\theta, \mathbb{Q})$ y sea $n = \text{gr}(p)$. Por la demostración del teorema A.6, los elementos $1 = \theta^0, \theta, \theta^2, \ldots, \theta^{n-1}$ forman una base de $\mathbb{Q}(\theta)$ sobre $\mathbb{Q}$, y como $\alpha \in \mathbb{Q}(\theta)$, entonces existen racionales únicos $c_0, c_1, \ldots, c_{n-1}$ tales que

$$\alpha = \sum_{i=0}^{n-1} c_i \theta^i =: r(\theta)$$

donde $r(x) = c_0 + c_1 x + \cdots + c_{n-1} x^{n-1} \in \mathbb{Q}[x]$.

Si $\theta = \theta_1, \theta_2, \ldots, \theta_n$ son los conjugados de θ, i.e. son las raíces de $p(x) = \text{Irr}(\theta, \mathbb{Q})$, pongamos

$$\alpha_k' := r(\theta_k), \quad 1 \leq k \leq n.$$

Note que el polinomio

$$f(x) = \prod_{i=1}^{n} (x - r(\theta_i))$$

es mónico y satisface que $f(\alpha) = 0$ ya que $\alpha = r(\theta) = r(\theta_1)$. Más aún, el polinomio $f(x)$ tiene coeficientes racionales ya que como $\alpha = r(\theta)$ y $\phi(x) = \text{Irr}(\alpha, \mathbb{Q})$, entonces $0 = \phi(\alpha) = \phi(r(\theta))$ y así el polinomio $g(x) = \phi(r(x))$, que tiene coeficientes en $\mathbb{Q}$ ya que ϕ y r están en $\mathbb{Q}[x]$, satisface que $g(\theta) = 0$. Entonces, como $p(x) = \text{Irr}(\theta, \mathbb{Q})$, por A.4 se sigue que $p(x)$ divide a $g(x)$ y por lo tanto todas las raíces $\theta_1, \ldots, \theta_n$ de $p(x)$ son raíces de $g(x) = \phi(r(x))$ y así los números $r(\theta_i)$ son raíces de $\phi(x) = \text{Irr}(\alpha, \mathbb{Q})$, i.e., los $r(\theta_i)$ son algunos de los α_j. Ahora, por el corolario A.3 aplicado a $\phi(x)$, para toda función simétrica $h \in \mathbb{Q}[x_1, \ldots, x_n]$ se tiene que $h(\alpha_1, \ldots, \alpha_n) \in \mathbb{Q}$, en particular para los α_i de la forma $r(\theta_j)$ se tiene que $h(r(\theta_1), \ldots, r(\theta_n)) \in \mathbb{Q}$; pero éstos son los coeficientes de $f(x)$, por el teorema de Viète, A.1, y por lo tanto $f(x) \in \mathbb{Q}[x]$ como se quería. Podemos entonces aplicar A.4 de donde se sigue que $\phi(x)$ divide a $f(x)$ ya que ϕ es el polinomio mónico de menor grado que se anula en α. Pongamos

$$f(x) = \phi(x)^s h(x)$$

con $s \geq 1$ entero y con ϕ y h coprimos (recuerde que ϕ es irreducible). Mostraremos que $h(x) = 1$ y para ésto observemos que como h es mónico, entonces basta mostrar que $h(x)$ es constante. Ahora, si $h(x)$ no fuera constante, entonces tendría una raíz y como $h(x) | f(x)$, esta raíz sería de la forma $r(\theta_t)$ para algún t. Así, $h(r(\theta_t)) = 0$, i.e., $h(r(x))$ se anula en θ_t, y como $p(x) = \text{Irr}(\theta, \mathbb{Q})$, entonces $p(x) | h(r(x))$ y por lo tanto $h(r(x))$ se anula en todos los ceros de $p(x)$, i.e., en todos los $\theta_1, \ldots, \theta_n$; en particular, en $\theta = \theta_1$ y así $0 = h(r(\theta)) = h(\alpha)$, i.e., α es raíz de $h(x)$, lo cual es imposible porque α es raíz de ϕ que es coprimo con h. Esta contradicción implica que $h(x)$ es

constante, como se quería. Se sigue que $h(x) = 1$ y por lo tanto $f(x) = \phi(x)^s$, por lo que $\mathrm{gr}(f) = s \cdot \mathrm{gr}(\phi)$, i.e., $n = sm$. Ahora, de $f(x) = \phi(x)^s$ se sigue que las raíces de $\phi(x)$ aparecen con multiplicidad s en $f(x)$, i.e., cada $\alpha_i' := r(\theta_i)$ raíz de $f(x)$ es un α_j repetido s veces. Así, todos los conjugados de α (los $\alpha_1, \ldots, \alpha_m$) son de la forma $r(\theta_i)$. Esta manera de expresar los conjugados de un número algebraico α es útil para mostrar que el conjugado de una suma o producto de números algebraicos es la suma o producto de los conjugados correspondientes, algo que no es obvio de la definición.

TEOREMA A.10. *Sean $\alpha, \beta \in \mathbb{C}$ números algebraicos y sean $\alpha_1, \ldots, \alpha_m$ y $\beta_1, \ldots, \beta_r$ sus conjugados respectivos. Sea $\theta \in \mathbb{C}$ tal que*

$$\mathbb{Q}(\alpha_1, \ldots, \alpha_m, \beta_1, \ldots, \beta_r) = \mathbb{Q}(\theta)$$

y sean $\theta_1, \ldots, \theta_n$ los conjugados de θ. Pongamos

$$\alpha = \sum_{i=0}^{n-1} c_i \theta^i =: r(\theta) \quad y \quad \beta = \sum_{i=0}^{n-1} d_i \theta^i =: t(\theta).$$

Denotemos con α' a cualquier conjugado de α, y similarmente para β. Entonces,

(1) *Los conjugados de $\alpha + \beta$ son de la forma $(\alpha + \beta)' = \alpha' + \beta'$.*

(2) *Los conjugados de $\alpha\beta$ son de la forma $(\alpha \cdot \beta)' = \alpha' \cdot \beta'$.*

(3) *Si $r \in \mathbb{Q}$, entonces tiene un único conjugado, r mismo.*

Demostración. Para la parte (1), como

$$\alpha + \beta = \sum_{i=0}^{n-1} c_i \theta^i + \sum_{i=0}^{n-1} d_i \theta^i = \sum_{i=0}^{n-1} (c_i + d_i)\theta^i = r(\theta) + t(\theta) = (r + t)(\theta),$$

entonces, por lo observado previamente al enunciado del corolario:

$$(\alpha + \beta)' = (r + t)(\theta_k) = r(\theta_k) + t(\theta_k) = \alpha_k' + \beta_k' = \alpha' + \beta'.$$

Similarmente para la parte (2),

$$(\alpha \cdot \beta)' = (r \cdot t)(\theta_k) = r(\theta_k) \cdot t(\theta_k) = \alpha_k' \cdot \beta_k' = \alpha' \cdot \beta'.$$

Para (3), note que $\mathrm{Irr}(r, \mathbb{Q}) = x - r$. □

Enteros algebraicos. Un número complejo $\alpha \in \mathbb{C}$ se dice que es un *entero algebraico* si existe un polinomio $f(x)$, mónico y con coeficientes enteros, tal que $f(\alpha) = 0$. Por ejemplo, todo entero $n \in \mathbb{Z}$ es un entero algebraico ya que es raíz del polinomio mónico $x - n \in \mathbb{Z}[x]$. De hecho, se tiene que:

LEMA A.11. *Un racional $r \in \mathbb{Q}$ es entero algebraico si y sólo si $r \in \mathbb{Z}$.*

Demostración. Sólo falta probar la suficiencia. Supongamos que $r = c/d \in \mathbb{Q}$ es un entero algebraico y que $\text{mcd}(c,d) = 1$. Entonces, existe un polinomio mónico $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 \in \mathbb{Z}[x]$ tal que $f(r) = 0$. Substituyendo $r = c/d$ en $f(x)$ y multiplicando por d^n obtenemos

$$c^n + a_{n-1}c^{n-1}d + + \cdots + a_0d^n = 0$$

por lo que $d|c^n$ y como son coprimos esto implica que $d = \pm 1$, por lo que $r = \pm c \in \mathbb{Z}$. □

Mostraremos a continuación que si α, β son enteros algebraicos, entonces $\alpha \pm \beta$ y $\alpha\beta$ también lo son. Para ésto necesitaremos el lema siguiente:

LEMA A.12. *Sean $n \geq 1$ un entero y $\xi \in \mathbb{C}$. Supongamos que los números complejos $\theta_1, \ldots, \theta_n$ no son todos cero y que satisfacen las ecuaciones*

$$(*) \qquad \xi\theta_j = a_{j1}\theta_1 + a_{j2}\theta_2 + \cdots + a_{jn}\theta_n, \quad (1 \leq j \leq n)$$

con los $a_{ji} \in \mathbb{Z}$. Entonces, ξ es un entero algebraico.

Demostración. Note que $(*)$ es un sistema de n ecuaciones lineales homogéneas en las n variables θ_j, y como por hipótesis tiene una solución no trivial, entonces el determinante del sistema es cero, i.e.,

$$0 = \det \begin{pmatrix} (\xi - a_{11}) & -a_{12} & \cdots & -a_{1n} \\ -a_{21} & (\xi - a_{22}) & \cdots & -a_{2n} \\ \vdots & & \ddots & \vdots \\ -a_{n1} & -a_{n2} & \cdots & (\xi - a_{nn}) \end{pmatrix} = \xi^n + b_n\xi^{n-1} + \cdots + b_1\xi + b_0$$

donde al desarrollar el determinante los coeficientes b_i son polinomios en las a_{jk} y por lo tanto $b_i \in \mathbb{Z}$ y como ξ es raíz del polinomio mónico con coeficientes enteros b_i, entonces ξ es un entero algebraico. □

TEOREMA A.13. *Si $\alpha, \beta \in \mathbb{C}$ son enteros algebraicos, entonces también lo son $\alpha \pm \beta$ y $\alpha\beta$.*

Demostración. Supongamos que α y β son raíces de los polinomios

$$f(x) = x^m + a_{m-1}x^{m-1} + \cdots + a_1x + a_0 \quad \text{y} \quad g(x) = x^n + b_{n-1}x^{n-1} + \cdots + b_1x + b_0$$

con los $a_i, b_j \in \mathbb{Z}$. Sea $t = mn$ y sean $\theta_1, \ldots, \theta_t \in \mathbb{C}$ dados por los $\theta_j = \alpha^r\beta^s$, para $0 \leq r \leq m-1$ y $0 \leq s \leq n-1$. Entonces, para todo j se tiene que

$$\alpha\theta_j = \alpha^{r+1}\beta^s = \begin{cases} \text{algún } \theta_k & \text{si } r+1 \leq m-1, \\ (-a_{m-1}\alpha^{m-1} - \cdots - a_1\alpha - a_0)\beta^s & \text{si } r+1 = m, \end{cases}$$

donde la segunda igualdad se obtiene despejando de $f(\alpha) = 0$ al término α^m.

Así, en ambos casos se ve que existen enteros $h_{j1}, \ldots, h_{jt}$ tales que

$$\alpha\theta_j = h_{j1}\theta_1 + \cdots + h_{jt}\theta_t.$$

En forma análoga se ve que existen enteros $\ell_{j1}, \ldots, \ell_{jt}$ tales que

$$\beta\theta_j = \ell_{j1}\theta_1 + \cdots + \ell_{jt}\theta_t$$

y por lo tanto

$$(\alpha \pm \beta)\theta_j = (h_{j1} \pm \ell_{j1})\theta_1 + \cdots + (h_{jt} \pm \ell_{jt})\theta_t,$$

con los $h_{ji} \pm \ell_{ji} \in \mathbb{Z}$. Del lema anterior se sigue que $\alpha \pm \beta$ es entero algebraico.

Similarmente, para el producto

$$\begin{aligned}(\alpha\beta)\theta_j = \alpha(\beta\theta_j) &= \alpha(\ell_{j1}\theta_1 + \cdots + \ell_{jt}\theta_t) = \ell_{j1}(\alpha\theta_1) + \cdots + \ell_{jt}(\alpha\theta_t) \\ &= \ell_{j1}(h_{11}\theta_1 + \cdots + h_{1t}\theta_t) + \cdots + \ell_{jt}(h_{t1}\theta_1 + \cdots + h_{tt}\theta_t) \\ &= k_{j1}\theta_1 + \cdots + k_{jt}\theta_t,\end{aligned}$$

con los $k_{ji} \in \mathbb{Z}$, y así del lema anterior se sigue que $\alpha\beta$ es un entero algebraico. □

Por su definición, los enteros algebraicos son números algebraicos, por lo tanto, si $\alpha \in \mathbb{C}$ es un entero algebraico, sea $p(x) = \operatorname{Irr}(\alpha, \mathbb{Q})$ el mónico irreducible del cual α es raíz (A.4). Mostraremos que $p(x)$ tiene coeficientes enteros y para ésto necesitaremos un lema debido a Gauss que esencialmente nos dice que irreducibilidad de un polinomio en $\mathbb{Z}[x]$ es equivalente a irreducibilidad en $\mathbb{Q}[x]$. Para probar este lema usaremos el concepto siguiente: el *contenido* de un polinomio $g(x) = b_0 + b_1x + \cdots + b_mx^m \in \mathbb{Z}[x]$ es $c(g) := \operatorname{mcd}(b_0, \ldots, b_m)$. Un polinomio $f(x) = a_0 + a_1x + \cdots + a_nx^n \in \mathbb{Z}[x]$ se dice que es *primitivo* si su contenido $c(g) = 1$. Observemos ahora que cualquier polinomio $g(x) \in \mathbb{Z}[x]$ se puede escribir de la forma $g(x) = df(x)$ con $d = c(g)$ y $f(x)$ primitivo, simplemente factorizando el mcd de los coeficientes de $g(x)$.

LEMA A.14 (Gauss). (1) *Si $f(x)$, $g(x)$ en $\mathbb{Z}[x]$ son primitivos, entonces su producto $f(x)g(x)$ también es primitivo.*

(2) *Si un polinomio $f(x) \in \mathbb{Z}[x]$ es irreducible, entonces considerado como polinomio en $\mathbb{Q}[x]$ también es irreducible.*

Obsérvese que como, obviamente, si $f(x)$ es irreducible en $\mathbb{Q}[x]$ también es irreducible en $\mathbb{Z}[x]$, entonces el lema de Gauss de hecho dice: *$f(x) \in \mathbb{Z}[x]$ es irreducible en $\mathbb{Z}[x]$ si y sólo si $f(x)$ es irreducible en $\mathbb{Q}[x]$.*

Demostración. (1) Si $f(x) = a_0 + a_1x + \cdots + a_mx^m$ y $g(x) = b_0 + b_1x + \cdots + b_nx^n$, $a_i, b_j \in \mathbb{Z}$, supongamos que $f(x) \cdot g(x) = c_0 + c_1x + \cdots + c_rx^r$ no es primitivo. Entonces, $\operatorname{mcd}(c_0, \ldots, c_r) = d > 1$, y así existe un primo $p \in \mathbb{Z}$ tal que $p|c_k$ para todos los $k = 0, \ldots, r$. Ahora, como $f(x)$ es primitivo, este primo p no divide a todos

los coeficientes a_i. Sea pues a_s el primer coeficiente de $f(x)$ no divisible por p. Similarmente, sea b_t el primer coeficiente de $g(x)$ no divisible por p. Consideremos ahora al coeficiente c_{s+t} de $f(x)g(x)$:

$$\begin{aligned} c_{s+t} &= (a_0b_{s+t} + a_1b_{s+t-1} + \cdots + a_{s-1}b_{t+1}) + a_sb_t \\ &\quad + (a_{s+1}b_{t-1} + a_{s+2}b_{t-2} + \cdots + a_{s+t}b_0) \end{aligned}$$

y obsérvese que como $p|a_i$, $0 \leq i \leq s-1$, entonces p divide al primer paréntesis en la ecuación de arriba, y similarmente p divide al segundo paréntesis. Y como por hipótesis $p|c_{s+t}$, entonces p debe dividir a a_sb_t, en contradicción con el hecho de que p no divide a a_s ni a b_t.

(2) Supongamos primero que $f(x) \in \mathbb{Z}[x]$ es primitivo. Si $f(x) = p(x)q(x)$, con $p(x)$ y $q(x)$ en $\mathbb{Q}[x]$, escribamos

$$p(x) = a_0/b_0 + (a_1/b_1)x + \cdots + (a_m/b_m)x^m,$$

con $a_i/b_i \in \mathbb{Q}$, y

$$q(x) = a'_0/b'_0 + (a'_1/b'_1)x + \cdots + (a'_n/b'_n)x^n$$

con $a'_i/b'_i \in \mathbb{Q}$. Si $b = b_0b_1 \cdots b_m$ y $b' = b'_0b'_1 \cdots b'_n$, entonces $p(x) = (1/b)b \cdot p(x)$ y $q(x) = (1/b')b' \cdot q(x)$, con $b \cdot p(x)$ y $b' \cdot q(x)$ en $\mathbb{Z}[x]$. Más aún, si d es el contenido de $b \cdot p(x)$ y d' es el contenido de $b' \cdot q(x)$, entonces $b \cdot p(x) = d \cdot u(x)$ y $b' \cdot q(x) = d' \cdot v(x)$ con $u(x), v(x) \in \mathbb{Z}[x]$ primitivos. Se sigue que

$$\begin{aligned} f(x) &= p(x) \cdot q(x) = \frac{1}{b}(d \cdot u(x)) \cdot \frac{1}{b'}(d' \cdot v(x)) \\ &= \frac{dd'}{bb'} \cdot u(x)v(x) = \frac{s}{t} \cdot u(x)v(x) \end{aligned}$$

y así

$$t \cdot f(x) = s \cdot u(x)v(x)$$

y como $f(x)$ es primitivo, entonces $c(t \cdot f(x)) = t$, y también, como $u(x)$ y $v(x)$ son primitivos, por la parte (1) el producto $u(x)v(x)$ es primitivo y así $c(s \cdot u(x)v(x)) = s$. Se sigue que $t = c(t \cdot f(x)) = c(s \cdot u(x)v(x)) = s$, i.e., $s = t$ y por lo tanto

$$f(x) = u(x) \cdot v(x)$$

con $u(x), v(x) \in \mathbb{Z}[x]$.

Finalmente, si $f(x) \in \mathbb{Z}[x]$ no es primitivo, escribamos $f(x) = d \cdot g(x)$ con $g(x) \in \mathbb{Z}[x]$ primitivo. Si $f(x)$ se factoriza en $\mathbb{Q}[x]$ como $f(x) = p(x)q(x)$, entonces $d \cdot g(x) = f(x) = p(x)q(x)$ y así

$$g(x) = \left(\frac{1}{d}p(x)\right)q(x)$$

con $(1/d) \cdot p(x), q(x) \in \mathbb{Q}[x]$, y entonces por la primera parte de la demostración, como $g(x)$ es primitivo, entonces $g(x) = u(x)v(x)$ con $u(x), v(x) \in \mathbb{Z}[x]$. Se sigue que $f(x) = d \cdot g(x) = (d \cdot u(x))v(x)$ con $d \cdot u(x), v(x) \in \mathbb{Z}[x]$. □

COROLARIO A.15. *Si $\alpha \in \mathbb{C}$ es un entero algebraico, entonces* $\mathrm{Irr}(\alpha, \mathbb{Q})$ *tiene coeficientes enteros.*

Demostración. Como α es entero algebraico, por el principio del buen orden, existe un mónico de menor grado $\phi(x) \in \mathbb{Z}[x]$ del cual α es raíz. Entonces, $\phi(x)$ es irreducible en $\mathbb{Z}[x]$ ya que si no lo fuera, existirían $f(x), g(x) \in \mathbb{Z}[x]$ mónicos tales que $\phi = fg$ con $1 \leq \mathrm{gr}(f), \mathrm{gr}(g) < \mathrm{gr}(\phi)$, y como $0 = \phi(\alpha) = f(\alpha)g(\alpha)$, entonces α sería raíz de un mónico en $\mathbb{Z}[x]$ de menor grado que el de ϕ, una contradicción. Así, $\phi(x)$ es irreducible en $\mathbb{Z}[x]$ y por el lema de Gauss se sigue que $\phi(x)$ es irreducible en $\mathbb{Q}[x]$. Por A.4 se sigue que $\mathrm{Irr}(\alpha, \mathbb{Q}) = \phi(x)$ y por lo tanto $\mathrm{Irr}(\alpha, \mathbb{Q}) \in \mathbb{Z}[x]$, como se quería. □

Notas. Los resultados sobre conjugados pueden ser demostrados, en forma más elegante, usando los elementos de la teoría de Galois, la cual captura, en forma sutil y económica, la acción del grupo simétrico sobre las raíces de un polinomio dado. Similarmente, el hecho de que los enteros algebraicos forman un anillo se puede demostrar usando la teoría de anillos conmutativos. Las demostraciones que hemos dado se encuentran, con pequeñas variaciones, en [7] y [15].

EJERCICIO 1. Muestre que la suma y producto de números algebraicos es algebraico. De hecho, demuestre que, con las operaciones de $\mathbb{C}$, el conjunto de números algebraicos es un campo.

EJERCICIO 2. Si $\alpha \in \mathbb{C}$ es un entero algebraico, demuestre que el grupo aditivo $\mathbb{Z}[\alpha]$ de los polinomios en α con coeficientes enteros, tiene un número finito de generadores.

EJERCICIO 3. Si $\alpha \in \mathbb{C}$ es algebraico, demuestre que existe un entero $n \neq 0$ tal que $n\alpha$ es entero algebraico.

EJERCICIO 4. Si α y β son enteros algebraicos, demuestre que las soluciones de $x^2 + \alpha x + \beta = 0$ también son enteros algebraicos.

EJERCICIO 5. Generalice el ejercicio anterior.

EJERCICIO 6. Si $\omega \in \mu_n$, demuestre que $\sum_{1 \leq i \leq n,\ \mathrm{mcd}(i,n)=1} \omega^i$ es un entero algebraico.

Sugerencia: Use inducción sobre n y note que el caso $\omega = 1$ es trivial. Para $n > 1$ note que ω es raíz de $x^{n-1} + \cdots + x + 1$.

Bibliografía

Libros:

(1) Barrera, F., *Introducción a la teoría de grupos*. SMM-Universidad Autónoma del Estado de Hidalgo, México, 2004.

(2) Burnside, W., *Theory of Groups of Finite Order*. Second Edition. Dover, New York, 2004.

(3) Cárdenas, H. y Lluis, E., *Módulos semisimples y representación de grupos finitos*. Trillas, México, 1970.

(4) Carmichael, R. D., *Introduction to the Theory of Groups of Finite Order*. Ginn & Co., Boston, 1937.

(5) Curtis, C. and Reiner, I., *Representation theory of finite groups and associative algebras*. AMS Chelsea, New York, 2006.

(6) Hall, M., *The Theory of Groups*. AMS Chelsea, New York, 1999.

(7) Hecke, E., *Vorlesungen über der Theorie der Algebraische Zahlen*. Chelsea, New York, 1970.

(8) Hungerford, T. W., *Algebra*. Springer Verlag, New York, 1997.

(9) Huppert, B., *Endliche Gruppen I*. Springer Verlag, Berlin, 1967.

(10) Isaacs, M., *Character theory of finite groups*. Academic Press, San Diego, 1976.

(11) Jordan, C., *Traité des substitutions et des équations algébriques*. Gauthier-Villars, Paris, 1870. Deuxiéme Edition. Paris, 1957. Réimpression, Jacques Gabay, 1989.

(12) Kurosh, A. G., *The Theory of Groups, 2 volumes*. Chelsea, New York, 1956.

(13) Kurzweil, H. and Stellmacher, B., *The Theory of Finite Groups. An Introduction*. Springer Verlag, New York, 2004.

(14) Pineda, M., *Aritmética y teoría de grupos*. UAM, México, 1995.

(15) Pollard, H. and Diamond, H. G., *The Theory of Algebraic Numbers*. Second Edition. The Carus Mathematical Monographs, MAA, Boston, 1975.

(16) Rotman, J. J., *The Theory of Groups. An Introduction*. Second Edition. Allyn and Bacon, Boston, 1978. (Fourth Edition: *An introduction to the theory of groups*. Springer Verlag, New York, 1999).

(17) Serre, J.-P., *Linear Representations of Finite Groups*. Springer Verlag, New York, 1999.

(18) Weyl, H., *La Simetría*. Nueva Visión, Buenos Aires, 1958.

(19) Wussing, H., *The genesis of the abstract group concept: A contribution to the history of the origin of abstract group theory*. MIT Press, Cambridge, MA, 1984.

Bibliografía

Libros:

(1) Barrera, F., *Introducción a la teoría de grupos*. SMM-Universidad Autónoma del Estado de Hidalgo, México, 2004.

(2) Burnside, W., *Theory of Groups of Finite Order*. Second Edition. Dover, New York, 2004.

(3) Cárdenas, H. y Lluis, E., *Módulos semisimples y representación de grupos finitos*. Trillas, México, 1970.

(4) Carmichael, R. D., *Introduction to the Theory of Groups of Finite Order*. Ginn & Co., Boston, 1937.

(5) Curtis, C. and Reiner, I., *Representation theory of finite groups and associative algebras*. AMS Chelsea, New York, 2006.

(6) Hall, M., *The Theory of Groups*. AMS Chelsea, New York, 1999.

(7) Hecke, E., *Vorlesungen über der Theorie der Algebraische Zahlen*. Chelsea, New York, 1970.

(8) Hungerford, T. W., *Algebra*. Springer Verlag, New York, 1997.

(9) Huppert, B., *Endliche Gruppen I*. Springer Verlag, Berlin, 1967.

(10) Isaacs, M., *Character theory of finite groups*. Academic Press, San Diego, 1976.

(11) Jordan, C., *Traité des substitutions et des équations algébriques*. Gauthier-Villars, Paris, 1870. Deuxiéme Edition. Paris, 1957. Réimpression, Jacques Gabay, 1989.

(12) Kurosh, A. G., *The Theory of Groups, 2 volumes*. Chelsea, New York, 1956.

(13) Kurzweil, H. and Stellmacher, B., *The Theory of Finite Groups. An Introduction*. Springer Verlag, New York, 2004.

(14) Pineda, M., *Aritmética y teoría de grupos*. UAM, México, 1995.

(15) Pollard, H. and Diamond, H. G., *The Theory of Algebraic Numbers*. Second Edition. The Carus Mathematical Monographs, MAA, Boston, 1975.

(16) Rotman, J. J., *The Theory of Groups. An Introduction*. Second Edition. Allyn and Bacon, Boston, 1978. (Fourth Edition: *An introduction to the theory of groups*. Springer Verlag, New York, 1999).

(17) Serre, J.-P., *Linear Representations of Finite Groups*. Springer Verlag, New York, 1999.

(18) Weyl, H., *La Simetría*. Nueva Visión, Buenos Aires, 1958.

(19) Wussing, H., *The genesis of the abstract group concept: A contribution to the history of the origin of abstract group theory*. MIT Press, Cambridge, MA, 1984.

(20) Zaldívar, F., *Teoría de Galois*. Anthropos, Barcelona, 1986.
(21) Zaldívar, F., *Fundamentos de álgebra*. FCE, México, 2005.

Artículos:

(22) Artin, E., *The Orders of the Linear Groups*. Comm. Pure and Applied Math. **8** (1955), 355-365. Collected Papers, 387-397.
(23) Bender, H., *A group-theoretical proof of the p^aq^b-theorem*. Math. Z. **126** (1972), 327-338.
(24) Brewster, B. and Ward, M., *Sylow Fractals*. Math. Magazine **68** (1975), 372-376.
(25) Burnside, W., *On groups of order $p^\alpha q^\beta$*. Proc. London Math. Soc. (2) **1** (1904), 388-392.
(26) Burnside, W., *On transitive subgrupos of degree n and class n − 1*. Proc. London Math. Soc. **23** (1900), 240-246.
(27) Cauchy, A., *Mémoire sur les arrangements que l'on peut former avec des lettres donneés et sur les permutations ou substitutions a l'aide desquelles on passe d'un arrangement a un autre*. Exercises d'Analyse et de Physique Mathématique. Tome III. (1844), 171-282 (Especialmente, pág. 192-196, para la *fórmula de Cauchy* y pág. 280 para el *teorema de Cauchy*). Œuvres Complètes. II^e Série. Tome XIII. Gauthier-Villars. Deuxiéme Edition. Paris, 1932.
(28) Cauchy, A., *Mémoire sur diverses propriétés remarquables des substitutions régulaires ou irrégulaires, et des systèmes de substitutions conjuguées*. C. R. Acad. Sci. Paris, **21** (1845), 972-98. Œuvres Complètes. Série I. Tome IX, 371-387 (Especialmente, pág. 386, para la *el teorema de Frobenius en el caso transitivo*). Gauthier-Villars. Deuxiéme Edition. Paris, 1932.
(29) Cayley, A., *On the theory of groups, as depending on the symbolic equation $\theta^n = 1$*. Philosophical Magazine and Journal of Science, Series 4, **7** (1854).
(30) Cayley, A., *Desiderata and Suggestions: No. 1. The Theory of Groups*. Am. Journal of Math. **1** (1878), 50-52.
(31) Dieck, W., *Gruppentheorische Studien*. Math. Ann. **20** (1882), 1-44.
(32) Feit, W. and Thompson, J. G., *Solvability of groups of odd order*. Pacific J. Math. **13** (1963), 775-1029.
(33) Frobenius, F. G., *Neuer Beweis des Sylowschen Satzes*. J. für die Reine und Angew. Math. **100** (1887), 179-181. Ges. Abh. II, 301-303.
(34) Frobenius, F. G., *Über die Congruenz nach einem aus zwei endlichen Gruppen gebildeten Doppelmoduln*. J. für die Reine und Angew. Math. **101** (1887), 273-299. Ges. Abh. II, Springer Verlag, Heidelberg (1988), 304-330.
(35) Frobenius, F. G., *Über Gruppencharaktere*. S'ber. Preuß. Akad. Wiss. Berlin. (1896), 985-1021. Ges. Abh. III, 1-37.

(36) Frobenius, F. G., *Über die Darstellung der endlichen Gruppen durch lineare Substitutionen*. S'ber. Preuß. Akad. Wiss. Berlin. (1897), 944-1015. Ges. Abh. III, 82-103.

(37) Frobenius, F. G., *Über Relationen zwischen den Charakteren einer Gruppe und denen ihrer Untergruppen*. S'ber. Preuß. Akad. Wiss. Berlin. (1898), 501-515. Ges. Abh. III, 104-118.

(38) Frobenius, F. G., *Über auflösbare Gruppen IV*. S'ber. Preuß. Akad. Wiss. Berlin. (1901), 1216-1230. Ges. Abh. III, 189-203

(39) Frobenius, F. G., *Über Gruppen der Ordnung* $p^{\alpha}q^{\beta}$. Acta Mathematica **26** (1902), 189-198. Ges. Abh. III, 210-219..

(40) Galois, É., *Mémoire sur les conditions de résolubilité des équations par radicaux*. (1831), 43-72. Écrits et Mémoirs Mathématiques d' Évariste Galois. Édition critique intégrale de ses manuscrits et publications, par R. Bourgne et J.-P. Azra. Gauthier-Villars. Paris, 1962.

(41) Grün, O., *Beiträge zur Gruppentheorie II. Über einen Satz von Frobenius*. J. für die Reine und Angew. Math. **186** (1945), 165-169.

(42) Hölder, O., *Zurückführung einer beliebigen algebraischen Gleichung auf eine Kette von Gleichungen*. Math. Ann. **34** (1889), 26-56. (Especialmente, pág. 33).

(43) Hölder, O., *Die einfachen Gruppen im ersten und zweiten Hundert der Ordnungszahlen*, Math. Ann. **40** (1892), 5588.

(44) Hölder, O., *Die Gruppen der Ordnungen* p^3, pq^2, pqr, p^4. Math. Ann. **43** (1893), 301-412.

(45) Jordan, C., *Sur les groupes d' ordre* $p^m q^2$. Liouville Journal **4** (1898), 21-26.

(46) Kaloujnine, L., *La structure des p-groups de Sylow des groups symétriques finis*. Ann. Sci. École Norm. Sup. **65** (1948), 239-276.

(47) Kronecker, L., *Auseinandersetzung einiger Eigenschaften der Klassenzahl idealer complexer Zahlen*. Monatsb. König. Preuß. Akad. Wiss. Berlin, (1870), 881-889. Werke I, Leipzig, (1895), 271-282.

(48) Lagrange, J.-L., *Refléxions sur la résolution algébrique des équations*. Œuvres de Lagrange, publiées par J.-A. Serret. Tome III, No. 99, 205-421. Gauthier-Villars. Paris, 1869.

(49) Nelson, S., *Defining the Sign of a Permutation*. Amer. Math. Monthly **94** (1987), 543-545.

(50) Picard, S., *Sur les bases du groupe symmétrique et du groupe alternant*. Ann. Math. **116** (1939), 752-767.

(51) Schreier, O., *Über die Erweiterung von Gruppen I*. Monats. Math. Phys. **34** (1926), 165-180.

(52) Schur, I., *Neue Begründung der Theorie der Gruppencharaktere*. S'ber. Preuß. Akad. Wiss. Berlin, (1905), 406-432. Ges. Abh. I, 143-169.

(53) Shaw, R. H., *Remark on a theorem of Frobenius*. Proc. A. M. S. **3** (1952), 970-972.

(54) Sylow, M. L., *Théoremès sur les groupes de substitutions*. Math. Ann. **5** (1872), 584-594.

(55) Weber, H., *Beweis des Satzes, dass jede eigentlich primitive quadratische Form unendlich viele Primzahlen darzustellen fähig ist*. Math. Ann. **20** (1882), 301-329.

(56) Weber, H., *Die allgemeinen Grundlagen der Galois'schen Gleichungstheorie*. Math. Ann. **43** (1893), 521-549.

(57) Wielandt, H., *Ein Beweis für die Existenz der Sylowgruppen*. Arch. Math. **10** (1959), 401-402.

Índice alfabético

acción, 2, 5, 97
  G-lineal, 170
  transitiva, 105, 238
  lineal, 170
  por conjugación, 98
  por traslación
    derecha por el inverso, 98
    izquierda, 97
  trivial, 97
asociatividad, 7, 11

campo, 159
  finito, 159
carácter, 185
  de la representación regular, 187
  inducido, 217
  principal, 187
  virtual, 219
carácterer
  inducido, 216
centralizador, 19, 104
centro de un grupo, 19
ciclo, 32
clase
  de un grupo nilpotente, 147
clases
  de conjugación, 42, 69
  laterales
    derechas, 54
    izquierdas, 54
complemento de Frobenius, 224
componentes p-primarias, 93
congruencia
  derecha, 53
  izquierda, 53
conjugado, 42, 69
conmutador, 66
conmutatividad, 7
contraejemplo al teorema de Lagrange, 65

ecuación de clases, 108
elemento
  neutro, 11
elemento primitivo, 160
entero algebraico, 246
espacio
  G-invariante, 175
  estable o invariante, 175
estabilizador, 99
estructura cíclica, 43
exponente
  de un grupo, 92
extensión
  de campos, 241
extensión simple, 241

factores invariantes, 94
fórmula de Cauchy, 46
Fórmulas de Viète, 236
función
  de clases, 195

G-conjunto, 97
G-espacio vectorial, 170
generador, 22
generadores, 28
grado
  de un carácter, 185
grado de una representación, 172

grupo, 11
  abeliano, 13
  alternante, 39
  cíclico, 22
    finito, 24
    infinito, 23
  cociente, 59
  de Frobenius, 224
  de Klein, 64
  de simetrías, 11
  diédrico, 42
  finito, 14
  generado por, 28
  lineal
    proyectivo, 162
  lineal especial, 162
  lineal general, 161
  nilpotente, 147
  simétrico, 30
  simple, 115, 131
  soluble, 141

homomorfismo, 71
  canónico, 73
  de transferencia, 227, 229
  signo, 73

imagen
  directa, 73
  inversa, 73
índice de un subgrupo, 57
intervalo de naturales, 29
inverso, 11
isomorfismo, 75

lema
  de Gauss, 248
  de Schur, 181
ley de los exponentes, 21

matriz escalar, 162

núcleo, 74
  de Frobenius, 224
número algebraico, 240
neutro, 8
Noether
  primer teorema de isomorfismo, 77
  segundo teorema de isomorfismo, 80
  tercer teorema de isomorfismo, 81
normalizador, 109
notación aditiva, 21

operación, 6
  binaria, 6
órbita
  de una acción, 99
  de una permutación, 32
orden
  de un elemento, 26
  de un grupo, 14
ortogonalidad
  de caracteres, 189
  por columnas, 199
  por renglones, 198

p-grupo, 93, 109, 114
p-primario, 93
p-subgrupo de Sylow, 111
paridad, 37
partición de un entero, 44
permutación, 29
permutaciones
  disjuntas, 34
polinomios
  simétricos, 235
  simétricos elementales, 236
potencias de un elemento, 21
producto
  corona, 122
  semidirecto, 118
producto directo
  externo, 87, 88
  interno, 88, 89
producto interior de caracteres, 189
puntos fijos, 99

raíz primitiva, 160
representación
  fiel, 184
  inducida, 217
  irreducible o simple, 178
  lineal, 171
  por permutaciones, 174
  regular, 173
  signo, 173
  trivial, 172

representaciones
  isomorfas, 172

serie
  central inferior, 149
  central superior, 147
  de composición, 139
  normal, 139
signo de una permutación, 38, 50
simetría, 1, 6
subgrupo, 16
  conmutador, 66
  de Frattini, 157
  de isotropía, 99
  normal, 62
subrepresentación, 175
suma directa de representaciones, 177
Sylow
  primer teorema, 110
  segundo teorema, 111
  tercer teorema, 112
tabla de caracteres, 197
teorema
  $p^r q^s$ de Burnside, 133, 143, 215
  órbita-estabilizador, 100
  de Burnside-Wielandt, 152
  de Cauchy, 108
  de Cayley, 84
  de correspondencia, 65
  de Feit-Thompson, 153
  de Frobenius, 101, 219, 223
  de isomorfismo de Noether, 77
  de Jordan-Hölder, 140
  de Lagrange, 56
  de Maschke, 179
  de Sylow, 110–112
  fundamental de los grupos abelianos finitos, 94
tipo de una permutación, 44
transposición, 36
transvección, 163
traza, 185

512.4
Z22

Sociedad Matemática Mexicana

Junta Directiva de la Sociedad Matemática Mexicana 2006–2008:

Alejandro Díaz Barriga Casales	•	presidente
Fernando Brambila Paz	•	vicepresidente
Isidoro Gitler Goldwain	•	secretario general
Antonio Rivera Figueroa	•	secretario de actas
Silvia Alatorre Frenk	•	tesorera
Marcela Santillán Nieto	•	vocal
Víctor H. Ibarra Mercado	•	vocal

La Sociedad Matemática Mexicana fue fundada en el año de 1943. Entre sus tareas fundamentales destacan: Estimular y mantener el interés por la investigación matemática en México; publicar revistas científicas; contribuir al mejoramiento de los programas de estudio y la enseñanza de las matemáticas en el país; estimular la elaboración y publicación de libros de texto en matemáticas; organizar conferencias, reuniones, congresos y concursos de matemáticas; cooperar en la resolución de los problemas matemáticos que se presentan en el sector productivo del país, así como los que surgen en las investigaciones de otras ciencias; promover el convencimiento entre la sociedad mexicana de que las matemáticas son parte integral de la cultura básica y de las habilidades de uso cotidiano de la población.

correo electrónico: smm@smm.org.mx
http://www.smm.org.mx

Instituciones patrocinadoras de la Sociedad Matemática Mexicana:

- *Benemérita Universidad Autónoma de Puebla*
- *Centro de Investigación en Matemáticas, A. C.*
- *Centro de Investigación y de Estudios Avanzados*
- Consejo Nacional de Ciencia y Tecnología
- *Fundación Universidad de las Américas, Puebla*
- *Instituto Tecnológico Autónomo de México*
- *Instituto Tecnológico Superior de Lerdo, Durango*
- Secretaría de Educación Pública
  - Subsecretaría de Educación Básica
  - Subsecretaría de Educación Superior
- *Universidad de Guadalajara*
- *Universidad de Sonora*
- *Universidad Anáhuac del Norte S.C.*
- Universidad Autónoma del Estado de Hidalgo
- *Universidad Autónoma del Noreste, Saltillo, Coah.*
- *Universidad Autónoma de Nuevo León*
- Universidad Autónoma de Querétaro
- *Universidad Autónoma de San Luis Potosí*
- Universidad Autónoma Metropolitana
  - *Unidad Iztapalapa*
- Universidad Nacional Autónoma de México
  - Facultad de Ciencias
  - Instituto de Matemáticas
- *Universidad Panamericana*
- Universidad Pedagógica Nacional
- *Universidad Tecnológica de Tula Tepeji*

Se han distinguido con letra cursiva los Miembros Institucionales de la SMM.

PUBLICACIONES DEL INSTITUTO DE MATEMÁTICAS, UNAM:

MONOGRAFÍAS DEL INSTITUTO DE MATEMÁTICAS

1 *Localization in non commutative rings.* B. J. Mueller (1975).
2 *Teoría de los números algebraicos.* A. Díaz-Barriga, A. I. Ramírez-Galarza, F. Tomás (1975).
3 *Integrales de medida positiva.* G. Zubieta (1976).
4 *Rings with polynomial identities.* B. J. Mueller (1977).
5 *Grupos profinitos, grupos libres y productos libres.* L. Ribes (1977).
6 *Introducción a la teoría de las clases características en la geometría algebraica.* A. Holme (1978).
7 *Embeddings, projective invariants and classifications.* A. Holme (1979).
8 *The relative spectral sequence of Leray-Serre for fibrations pairs.* C. Prieto (1979).
9 *Caminatas aleatorias y movimiento browniano.* D. B. Hernández (1981).
10 *On polarized varieties.* T. Matsusaka (1981).
11 *Métodos diagramáticos en teoría de representaciones.* C. Cibils, F. Larrión, L. Salmerón (1982).
12 *Espacios simplécticos sobre β-anillos y anillos de Hermite, trasvecciones simplécticas.* E. Fernández Bermejo (1982).
13 *Abelian integrals.* G. Kempf (1983).
14 *On Selfinjective algebras of finite representation type.* J. Waschbüsch (1983).
15 *On ideal theory in Banach and topological algebras.* W. Zelazko (1984).
16 *Teoría general de procesos e integración estocástica.* T. Bojdecki (1985).
17 *La figura espectral de operadores.* C. Hernández Garciadiego, E. de Oteyza (1986).
18 *Teoría de punto fijo.* A. Dold. Traducción: C. Prieto. Vol. I, Vol. II, Vol. III (1986).
19 *Projective embeddings of algebraic varieties.* J. Roberts (1988).
20 *Teoría general de procesos e integración estocástica.* 2a. Edición. T. Bojdecki (1989).
21 *Análisis funcional I.* C. Bosch Giral, E. Fernández Bermejo (1989).
22 *Introducción a la topología de las variedades de dimensión infinita.* L. Montejano (1989).
23 *Introducción a la teoría de representaciones de álgebras.* R. Martínez-Villa (1990).

MEMORIAS DEL 50 ANIVERSARIO DEL INSTITUTO DE MATEMÁTICAS. 1942–1992.

MATEMÁTICAS EN LA UNAM. MEMORIAS DEL 60 ANIVERSARIO DEL INSTITUTO DE MATEMÁTICAS. (2003).

Topología algebraica. Un enfoque homotópico. M. Aguilar, S. Gitler, C. Prieto. Coedición de Instituto de Matemáticas, UNAM – McGraw-Hill Interamericana Editores (1998).

CUADERNOS DE OLIMPIADAS DE MATEMÁTICAS.

1 *Combinatoria.* M. L. Pérez-Seguí. 3a. edición (2005).
2 *Principios de olimpiada.* A. Illanes Mejía. 2a. Reimpresión de la 2a. edición (2006).
3 *Geometría.* R. Bulajich, J. A. Gómez Ortega. 4a. Reimpresión (2006).
4 *Geometría. Ejercicios y problemas.* R. Bulajich, J. A. Gómez Ortega. 4a. Reimpresión (2006).
5 *Teoría de números.* M.L. Pérez-Seguí. 3a. Reimpresión (2006).
6 *Desigualdades.* R. Bulajich, J.A. Gómez Ortega 2a. edición (2005).
12 *Inequalities.* R. Bulajich, J.A. Gómez Ortega (2005).

TEMAS DE MATEMÁTICAS PARA BACHILLERATO.

1 *Cuando cuentes cuántos...* H. A. Rincón Mejía (2002).
2 *Sistemas de ecuaciones y de desigualdades.* A. I. Ramírez Galarza (2002).
3 *La historia de un empujón: un vistazo a las ecuaciones diferenciales ordinarias y a los sistemas dinámicos.* L. Ortiz Bobadilla y E. Rosales González (2002).
4 *Dos o tres trazos.* S. Cárdenas Rubio (2003).
5 *Estadística descriptiva para bachillerato.* M.P. Alonso Reyes, J.A. Flores Díaz (2004).

6 *Relaciones de equivalencia.* M. Cruz Terán (2005).
7 *Mosaicos.* L. Hidalgo (por aparecer).

PUBLICACIONES DE LA SOCIEDAD MATEMÁTICA MEXICANA Y DEL INSTITUTO DE MATEMÁTICAS:

APORTACIONES MATEMÁTICAS

Serie: INVESTIGACIÓN

1 *Coloquio de sistemas dinámicos. Memorias. Guanajuato, México, 1983.* Editado por J. A. Seade, G. Sienra (1985).
2 *Categorical topology - The complete work of Graciela Salicrup.* Edited by H. Herrlich, C. Prieto (1988).
3 *Sistemas dinámicos holomorfos en superficies.* X. Gómez-Mont, L. Ortíz-Bobadilla. 2a. edición (2004).
4 *Simposio de probabilidad y procesos estocásticos. Memorias. Guanajuato, México 1988.* Editado por M. E. Caballero, L. G. Gorostiza (1989).
5 *Topics in algebraic geometry. Proceedings. Guanajuato, México 1989.* Editado por L. Brambila-Paz, X. Gómez-Mont (1992).
6 *Seminario internacional de álgebra y sus aplicaciones. Memorias. México 1991.* Editado por L. M. Tovar, C. Rentería, R. H. Villarreal (1992).
7 *II Simposio de probabilidad y procesos estocásticos. I Encuentro México-Chile de análisis estocástico. Memorias. Guanajuato, México 1992.* Editado por M. E. Caballero, L. G. Gorostiza (1992).
8 *Taller de geometría diferencial sobre espacios de geometrías. Memorias. Guanajuato, México 1992.* Editado por L. del Riego, C. T. J. Dodson (1992).
9 *Poblaciones aleatorias ramificadas y sus equilibrios.* A. Wakolbinger (1994).
10 *Una Introducción a la geometría computacional a través de los teoremas de la galería de arte.* V. Estivill-Castro (1994).
11 *III Simposio de probabilidad y procesos estocásticos. Memorias. Hermosillo, México 1994.* Editado por M. E. Caballero, L. G. Gorostiza (1994).
12 *IV Simposio de probabilidad y procesos estocásticos. Memorias. Guanajuato, México 1996.* Editado por L. G. Gorostiza, J. A. León, J. A. López-Mimbela (1996).
13 *Taller de variedades abelianas y funciones theta. Memorias. Morelia, Mich., México 1996.* Editado por R. Rodríguez, J. M. Muñoz Porras, S. Recillas (1998).
14 *Modelos estocásticos.* Editado por J. M. González Barrios, L. G. Gorostiza (1998).
15 *Inverse limits.* W. T. Ingram (2000).
16 *Modelos Estocásticos II.* Editado por D. Hernández, J. A. López-Mimbela, R. Quezada (2001).
17 *Topics in infinitely divisible distributions and Lévy processes.* A. Rocha-Arteaga, K. Sato (2003).
18 *Parametric Optimization and Related Topics VII.* Editado por J. Guddat, H. Th. Jongen, J.-J. Rückmann, M. Todorov (2004).

Serie: COMUNICACIONES

1 *Programa de investigación del XVIII congreso nacional de la Sociedad Matemática Mexicana. Memorias. Mérida, México 1984.* Editadas por M. Clapp, J. A. Seade (1986).
2 *Teoremas límite de alta densidad para campos aleatorios ramificados.* B. Fernández (1986).

3 *Programa del XIX congreso nacional de la Sociedad Matemática Mexicana, Vol. I. Memorias. Guadalajara, México 1986.* Editadas por J. A. de la Peña, C. Prieto, G. Valencia, L. Verde (1987).

4 *Programa del XIX congreso nacional de la Sociedad Matemática Mexicana, Vol. II. Memorias. Guadalajara, México 1986.* Editado por J. A. de la Peña, C. Prieto, G. Valencia, L. Verde (1987).

5 *Programa del XX congreso nacional de la Sociedad Matemática Mexicana. Memorias. Xalapa, México 1987.* Editado por M. A. Aguilar, L. Salmerón, C. Vargas (1988).

6 *XXI Congreso nacional de la Sociedad Matemática Mexicana. Memorias. Hermosillo, Sonora 1988.* Editado por F. Aranda, J. Bracho, A. Sánchez Valenzuela, A. Vargas (1989).

7 *Breve introducción a códigos detectores-correctores de error.* C. Rentería, H. Tapia, W. Y. Vélez (1990).

8 *XXII Congreso nacional de la Sociedad Matemática Mexicana. Memorias. Puebla, Puebla 1989.* Editado por P. Barrera, A. Illanes, F. O'Reilly, S. Recillas (1990).

9 *XXIII Congreso nacional de la Sociedad Matemática Mexicana. Memorias. Guanajuato, México 1990.* Editado por A. García-Máynez, L. G. Gorostiza, J. Ize, M. Mendoza (1991).

10 *La estructura de los dendroides suaves.* S. Macías Alvarez (1993).

11 *XXIV Congreso nacional de la Sociedad Matemática Mexicana. Memorias. Oaxtepec, Morelos 1991.* Editado por O. Hernández, L. Montejano, B. Rumbos, A. A. Wawrzyñzyk (1992).

12 *XXV Congreso nacional de la Sociedad Matemática Mexicana Vol. I. Memorias. Xalapa, Veracruz 1992.* Editado por F. Larrión, A. Olvera, V. Pérez-Abreu, E. Vallejo (1993).

13 *XXV Congreso nacional de la Sociedad Matemática Mexicana Vol. II. Memorias. Xalapa, Veracruz 1992.* Editado por F. Larrión, A. Olvera, V. Pérez-Abreu, E. Vallejo (1993).

14 *XXVI Congreso nacional de la Sociedad Matemática Mexicana. Memorias. Morelia, Mich. 1993.* Editado por M. E. Caballero, J. Delgado, A. G. Raggi, J. Rosenblueth (1994).

15 *XI Escuela Latinoamericana de Matemáticas. Memorias. UNAM, México, D. F.; CIMAT, Gto. 1993.* Editado por X. Gómez-Mont, J. A. de la Peña, J. A. Seade (1994).

16 *XXVII Congreso nacional de la Sociedad Matemática Mexicana. Memorias. Querétaro, Qro. 1994.* Editado por J. A. León, A. Nicolás, F. Ongay, A. Tamariz (1995).

17 *Grupo de estudio con la industria y cursos en matemáticas industriales. Memorias. Oaxaca, Oaxaca 1995.* Editado por A. Fitt, R. Martínez-Villa (1996).

18 *XXVIII Congreso nacional de la Sociedad Matemática Mexicana. Memorias. Colima, Colima 1995.* Editado por J. L. Morales Pérez, S. Pérez Esteva, F. Sánchez Bringas, G. Villa Salvador (1996).

19 *Problemas combinatorios sobre conjuntos finitos de puntos.* B. M. Ábrego Lerma (1997).

20 *XXIX Congreso nacional de la Sociedad Matemática Mexicana. Memorias. San Luis Potosí, SLP 1996.* Editado por F. Avila Murillo, R. Montes-de-Oca, R. del Río Castillo, J. Muciño-Raymundo (1997).

21 *IV Escuela de verano de geometría y sistemas dinámicos. Memorias. Cimat, Guanajuato 1997.* Editado por O. Calvo, R. Iturriaga (1998).

22 *XXX Congreso nacional de la Sociedad Matemática Mexicana. Memorias. Aguascalientes, Ags. 1997.* Editado por A. López Mimbela, M. Neumann, M. Rzedowski, M. Shapiro (1998).

23 *Segundo grupo de estudio con la industria y cursos en matemáticas industriales. Memorias. Cocoyoc, Mor., México. 1997.* Editado por A. Fitt, R. Martínez-Villa, H. Ockendon (1999).

24 *3rd. International conference on approximation and optimization in the Caribean. Proceedings. Puebla, México. 1995.* Editado por B. Bank, J. Bustamante, J. Guddat, M. A. Jiménez, H. Th. Jongen, W. Römisch (1998).

25 *XXXI Congreso nacional de la Sociedad Matemática Mexicana. Memorias. Hermosillo, Son. 1998.* Editado por P. Padilla, R. Quiroga, C. Signoret, A. Soriano (1999).

26 *Tendencias interdisciplinarias de las matemáticas.* Editado por S. Gitler, C. Prieto (2000).

27 *XXXII Congreso nacional de la Sociedad Matemática Mexicana. Memorias. Guadalajara, Jal. 1999.* Editado por L. Hernández Lamoneda, R. Quezada, J. Martínez Bernal, H. Sánchez Morgado (2000).

28 *Lecturas Básicas en Topología General.* Editado por L. M. Villegas, A. Sestier, J. Olivares (2000).

29 *XXXIII Congreso nacional de la Sociedad Matemática Mexicana. Memorias. Saltillo, Coah. 2000.* Editado por J. Alfaro, M. Eudave, J. González Espino-Barros, E. Pérez Chavela (2001).
30 *XXXIV Congreso Nacional de la Sociedad Matemática Mexicana. Memorias. Toluca, Méx. 2001.* Editado por G. Contreras, C. Rentería, E. R. Rodríguez, C. Villegas Blas (2002).
31 *Tópicos de Geometría Algebraica.* Editado por L. Brambila, P.L. del Angel, A. García Zamora, J. Muciño (2002).
32 *XXXV Congreso Nacional de la Sociedad Matemática Mexicana. Memorias. Durango, Dgo. 2002.* Editado por M. Aguilar, R. Quiroga (2003).
33 (Número cancelado.)
34 *XXXVI Congreso Nacional de la Sociedad Matemática Mexicana. Memorias. Pachuca, Hgo. 2003.* Editado por M. Aguilar, R. Quiroga (2004).
35 *Memorias de la Sociedad Matemática Mexicana.* Editado por M. Aguilar, R. Quiroga (2005).

Serie: TEXTOS

1 *Introducción a la topología - Graciela Salicrup.* Editado por J. Rosenblueth, C. Prieto. Nivel medio. 1a. Reimpresión (1997).
2 *Procesos estocásticos.* C. Tudor. Nivel avanzado. 3a. Edición (2002).
3 *Lectures on continuous-time Markov control processes.* O. Hernández-Lerma. Nivel avanzado (1994).
4 *Un curso de lógica matemática.* C. R. Videla. Nivel avanzado (1995).
5 *Rudimentos de mansedumbre y salvajismo en teoría de representaciones.* F. Larrión, A. G. Raggi, L. Salmerón. Nivel avanzado (1995).
6 *Teoría general de procesos e integración estocástica.* T. Bojdecki. Nivel avanzado. 1a. Reimpresión (2004).
7 *Intersection theory.* S. X. Descamps. Nivel avanzado (1996).
8 *Inverse problems.* H. W. Engl. Nivel avanzado (1996).
9 *El ABC de los splines.* P. Barrera, V. Hernández, C. Durán. Nivel elemental (1996).
10 *Lo antiguo y lo nuevo acerca de los conjuntos convexos.* H. Hadwiger. Traducción: L. Montejano. Nivel medio (1998).
11 *Matemáticas para las ciencias naturales.* J. L. Gutiérrez Sánchez, F. Sánchez Garduño. Niveles medio y avanzado (1998).
12 *Introducción a la teoría de redes.* M. C. Hernández Ayuso. Nivel medio 2a. Edición (2005).
13 *Teoría de conjuntos (una introducción).* F. Hernández Hernández. Nivel medio 2a. Edición (2003).
14 *Lectures on quantum probability.* A. M. Chebotarev. Nivel avanzado (2000).
15 *Construcción de procesos autosimilares con variancia finita.* J. E. Figueroa López. Nivel avanzado (2000).
16 *Grupos algebraicos y teoría de invariantes.* C. Sancho de Salas. Nivel avanzado (2001).
17 *Cohomología de Galois de campos locales.* F. Zaldívar. Nivel avanzado (2001).
18 *Dimension Theory: An Introduction with Exercises.* S.B. Nadler, Jr. Nivel avanzado (2002).
19 *Cómputo Numérico con aritmética de punto flotante IEEE. Con un teorema, una regla empírica y ciento un ejercicios.* M. L. Overton. Traducción: A. Casares Maldonado. Nivel medio (2002) **Coedición SIAM.**
20 *Topología Diferencial.* V. Guillemin, A. Pollack. Traducción: O. Palmas Velasco. Nivel medio (2003).
21 *Elementos de Probabilidad y Estadística.* A. Hernández-del-Valle, O. Hernández-Lerma. Nivel elemental (2003).
22 *Topología General.* D. Hinrichsen, J. L. Fernández Muñiz, A. Fraguela Collar, Á. Álvarez Prieto. Nivel medio (2003).
23 *Introducción a los grupos topológicos de transformaciones.* S. de Neymet U. Con la colaboración de R. Jiménez B. Nivel avanzado (2005).
24 *Breviario de teoría analítica de los números.* E. P. Balanzario. Nivel medio (2003).
25 *Cálculo de probabilidades.* F. M. Hernández Arellano. Nivel elemental (2003).
26 *Números primos y aplicaciones.* F. Luca. Nivel avanzado (2004).
27 *Historia y desarrollo de la teoría de los continuos indescomponibles.* F.L. Jones. Traducción: S. Macías. Nivel medio (2004).

28 *Hiperespacios de continuos.* A. Illanes. Nivel medio (2004).
29 *Cadenas de Markov.* M.E. Caballero, V.M. Rivero, G. Uribe Bravo, C. Velarde. Nivel medio (2004).
30 *The fixed point property for continua.* S.B. Nadler, Jr. Nivel avanzado (2005).
31 *Invitación a la teoría de los continuos y sus hiperespacios.* Editado por R. Escobedo, S. Macías, H. Méndez. Nivel medio (2006).
32 *Introducción a la teoría de grupos.* F. Zaldívar. Nivel medio (2006).
33 *Hyperspaces of sets. A text with research questions.* S.B. Nadler, Jr. Nivel avanzado (2006).

Las matemáticas y la imaginación. E. Kasner, J. Newman. Traducción: M. Lara, L. Gorostiza (2006).

Contemporary Mathematics

260 *First summer school in analysis and mathematical physics. Cuernavaca, Morelos, 1998.* Editado por S. Pérez-Esteva, C. Villegas-Blas. Contemporary Mathematics No. 260. Coedición de Aportaciones Matemáticas - American Mathematical Society (2000).
289 *Second summer school in analysis and mathematical physics. Cuernavaca, Morelos, 2000.* Editado por S. Pérez-Esteva, C. Villegas-Blas. Contemporary Mathematics No. 289. Coedición de Aportaciones Matemáticas - American Mathematical Society (2001).
336 *Stochastic Models.* Editado por J.M. González-Barrios, J.A. León, A. Meda. Contemporary Mathematics No. 336. Coedición de Aportaciones Matemáticas - American Mathematical Society (2003).
340 *Spectral Theory of Schrödinger Operators. Lecture Notes from a Workshop on Schrödinger Operator Theory. IIMAS, UNAM, Mexico, 2001.* Editado por Rafael del Río, Carlos Villegas-Blas. Contemporary Mathematics No. 340 Coedición de Aportaciones Matemáticas - American Mathematical Society (2004).
341 *Topological algebras and their applications. Fourth International Conference on Topological Algebras and Their Applications. Oaxaca, Mexico, 2002.* Editado por Hugo Arizmendi, Carlos Bosch, Lourdes Palacios. Contemporary Mathematics No. 341. Coedición de Aportaciones Matemáticas - American Mathematical Society (2004).
389 *Geometry and Dynamics International Conference in Honor of the 60th Anniversary of Alberto Verjovsky. January 6-11, 2003. Cuernavaca, Mexico.* Editado por James Eells, Etienne Ghys, Mikhail Lyubich, Jacob Palis, José Seade. Contemporary Mathematics No. 389. Coedición de Aportaciones Matemáticas - American Mathematical Society (2005).

OBRAS COMPLETAS DE DIEGO BRICIO HERNÁNDEZ CASTAÑOS

I *Formas cuadráticas y operadores lineales.* D. B. Hernández Castaños (1994).
II *Método Monte Carlo.* D. B. Hernández Castaños, L. J. Alvarez (1995).
III *Métodos matemáticos de la termodinámica.* D. B. Hernández Castaños, E. Cárdenas Cuenca, C. A. Rincón Orta, C. B. Velarde Velázquez (1996).
IV *Teoría del potencial.* L. Briseño, M. E. Caballero, D. B. Hernández Castaños (1998).

Información y pedidos:

Sra. Gabriela Sanginés, Depto. de Publicaciones
Instituto de Matemáticas, UNAM, Circuito Exterior
Ciudad Universitaria, 04510 México, D. F. MEXICO
TEL: (52) (5) 622-44-96,
FAX: (52) (5) 550 13 42 y (52) (5) 616 03 48
e-mail: edicion@matem.unam.mx
WEB: http://www.matem.unam.mx
http://www.smm.org.mx

Introducción a la teoría de grupos, se terminó de imprimir en el mes de septiembre de 2006 en los talleres de Creativa Impresores, SA de CV. Quetzalcoatl 69, Tlaxpana, México D.F. Tel. 5703 2241. El tiraje en papel gráfico bond de 90 gramos de 70×95 cm consta de 500 ejemplares en pasta rústica con acabado en lámina de plástico.

Apoyo técnico:

Depto. de Publicaciones
Instituto de Matemáticas, UNAM

Gabriela Sanginés, Leonardo Espinosa, Celia Osorio

APORTACIONES MATEMÁTICAS es una publicación de la Sociedad Matemática Mexicana. Su serie **TEXTOS** comprende libros de texto de matemáticas y sus aplicaciones, para la licenciatura y el posgrado en matemáticas y en otras disciplinas. Se divide en tres niveles:

- *Nivel elemental:*
  Dirigido a estudiantes de los primeros dos años de la licenciatura.
- *Nivel medio:*
  Dirigido a estudiantes de los dos últimos años de la licenciatura.
- *Nivel avanzado:*
  Dirigido a estudiantes de posgrado.

INTRODUCCIÓN A LA TEORÍA DE GRUPOS

de Felipe Zaldívar, es un texto de *nivel medio.*

Desde la geometría hasta la física, desde la combinatoria hasta la teoría de números, dondequiera que existan simetrías, la teoría de grupos está presente. Este libro es una introducción a la teoría de grupos, y a pesar que sólo es una introducción elemental, toca muchos aspectos de la teoría, con un énfasis en los grupos finitos, preparando al estudiante para niveles más avanzados. Los prerrequisitos para leer este libro se han mantenido a un mínimo: un curso de Álgebra Lineal y un curso de Matemáticas Finitas que incluya algo de divisibilidad de enteros, números primos y el teorema fundamental de la aritmética. El libro comienza con un intento de describir el concepto de *simetría* para motivar la idea de *grupo* y después de discutir algunos ejemplos importantes, grupos *cíclicos*, de *permutaciones* y de *matrices*, introduce los teoremas de estructura básicos, desde el teorema de Lagrange hasta los teoremas de Sylow, y luego los aplica para dar una introducción elemental al estudio de los grupos *simples* y *solubles*. La parte final del libro es una introducción a la teoría de caracteres de grupos finitos y luego aplica estos resultados para probar un importante teorema de Burnside, a saber, que todos los grupos finitos cuyos órdenes son de la forma $p^a q^b$, con p, q primos, son solubles.

Diseño de portada: Rubén Valencia.

REVERTÉ EDICIONES
ISBN 968-6708-66-9
9 789686 708660

ISBN 970-32-3871-8

BIBLIOTECA
FACULTAD DE CIENCIAS - UNI
0018215

Lista de errores tipográficos del libro *Introducción a la teoría de grupos*
de Felipe Zaldívar
SMM-Reverté, Primera reimpresión, 2009
Fecha de actualización: Junio, 2012

pág. 33, línea 18, debe decir $\text{orb}_\sigma(5) = \{5, 6\} = \text{orb}_\sigma(6)$

pág. 51, ejercicio 16, líneas -17 y -16, debe decir "manda el vértice v_1 a v_k,"

pág. 51, ejercicio 18, línea -9, dice "para $1 \leq i, j \leq n$", debe decir "para $1 \leq i, j < n$"

pág. 60, línea -14, antes del enunciado del teorema 5.9, dice "producto G/H", debe decir, "cociente G/H"

pág. 60, en la última línea del enunciado del teorema 5.9, dice "para todo $\sigma \in H$", debe decir "para todo $\sigma \in G$"

pág. 62, ejemplo 5, línea -1, dice "$A_3 = \{2, \sigma_3, \sigma_4\}$", debe decir "$A_3 = \{e, \sigma_3, \sigma_4\}$"

pág. 63, ejemplo 5, línea 8, dice "$eA_3 = \{2, \sigma_3, \sigma_4\}$", debe decir "$eA_3 = \{e, \sigma_3, \sigma_4\}$"

pág. 63, ejemplo 5, línea 11, dice "$A_3e = \{2, \sigma_3, \sigma_4\}$", debe decir "$A_3e = \{e, \sigma_3, \sigma_4\}$"

pág. 66, en la referencia en la primera nota al pie de página la revista es "Mathematics Magazine" **66** (1993), p.23.

pág. 68, línea 2, ejercicio 7, dice "todo subgrupo de K es normal en G", debe decir "todo subgrupo normal de K es normal en G".

pág. 75, línea 1, dice "es un subgrupo normal de G'", debe decir "es un subgrupo de G'"

pág. 85, línea 9, la referencia correcta en las **Notas** es: [30].

pág. 95, en los ejercicios 1, 2, y 3 se debe añadir la hipótesis de que los grupos considerados son finitos.

pág. 99, en el enunciado del lema 8.1 falta el punto final.

pág. 134, línea -6, debe decir "Los grupos A_1 y A_2" son triviales

pág. 144, línea 14, dice "proposición 5.15" debe decir "lema 5.13"

pág. 185, línea 14, dice $\text{Tr}(\rho(\sigma)) \in \mathbb{C}$, debe decir $\text{Tr}(\rho(g)) \in \mathbb{C}$

pág. 186, línea 13, dice $u_1, \ldots, u_r$, debe decir $u_1, \ldots, u_n$

pág. 189, línea 17, la segunda suma $\sum_{g\in G}$ debe ser $\sum_{g^{-1}\in G}$

pág. 191, línea 4, en la segunda suma los subíndices deben ser "$s, t, g \in G$"

pág. 193, línea -5, R cambia a ρ_R

pág. 194, línea 4, V_R cambia a $\rho_R : G \to \mathrm{GL}(V_R)$

pág. 195, línea 18, se cierra un paréntesis en el lado derecho de la fórmula desplegada.

pág. 196, línea 17, la igualdad $\rho_f = \sum \sigma \in Gf(\sigma)\rho(\sigma)$ debe ser $\rho_f = \sum_{\sigma\in G} f(\sigma)\rho(\sigma)$

pág. 197, línea 11, a la segunda suma le falta el factor $|C_\sigma|$ y debe ser

$$= \frac{1}{|G|} \sum_{g\in C_\sigma} |C_\sigma| \overline{\chi}_i(g) =$$

pág. 252, bibliografía, referencia [26] el título del artículo dice "subgrupos of" debe decir "subgroups of"

pág. 252, bibliografía, en la cuarta línea de la referencia [28] dice "la el teorema", debe decir "el teorema"